An E-commerce Agreement Based on the Points System of the Blockchain and the Secure Multi-party Platform

Jiayi Hu[1], Peifan Xin[2], Jiahui Deng[3], Jiawei Qian[*4]

[1]International school Jiangxi University of Finance and Economics. Nanchang, China
[2] School of Mathematics University of Leeds Leeds, United Kingdom
[3] International school Jiangxi University of Finance and Economics. Nanchang, China
[4] Computer science and software engineering East China Normal University, Shanghai, China

Abstract. Blockchain technology, as the supporting technology in digital currency, has brought considerable changes to e-commerce sector with its decentralised, tamper-proof and anonymous working methods. Based on the characteristics and the tamper-proof traceability of the block chain, this study constructs the application architecture of the e-commerce platform integration system, which not only realises the collaborative computing on the multi-party secure data platform, but also maintains the confidentiality of the calculation verification and input data. Additionally, the actual consumption process of consumers is introduced for case analysis to verify the feasibility of the method, which guides the collaborative application of blockchain technology and multi-party security computing technology in the field of e-commerce.

1 Introduction

Blockchain Technology is a technical solution that does not rely on third parties and uses its own distributed nodes to store, verify, transfer and communicate network data. Due to the features of blockchain, such as security and credibility, traceability and non-tampering, it can effectively prevent data from being tampered and avoid internal risks in the context of big data transaction, asset transaction and points circulation and exchange. Nevertheless, quite a few platforms cannot avoid the dilemma of how to compare the data size of two parties without a trusted third party. Multi-party secure computing (MPC) is aimed at the absence of a trusted third party. In a distributed network, multiple participating entities each hold secret inputs. Except for the calculation results, no input information from other participating entities can be obtained. At present, the most advanced technologies are obfuscation circuit, unintentional transmission and homomorphic encryption. Many scholars have conducted in-depth research on blockchain and multi-party computing. Literature[1] uses the arithmetic circuit to solve the problem of secure multi-party computation in a general sense. The computation and communication costs are linear with the input size. Literature [2] directly addresses the problem of millionaires and proposes a solution based on dazed transfer, which successfully solves the problem using simple XOR operations. Some scholars have applied the idea of homomorphic encryption to the problem of millionaires, and have also achieved good research results. Tzeng et al. [3] encoded natural numbers into a set, and reduced the size comparison problem to the set intersection problem. Based on this, Li et al. [4] reduced the comparison problem of two numbers to the secret calculation problem of partial scalar products of vectors. Zuo et al. [5] used the new protocol as the basic module based on the predecessors. They can query the sorting problem of the data in the ordered set at one time without comparing the data multiple times. Christian [6] proposed a collaborative data platform to detect and prevent disease for citizens; Kaw, Javaid A. [7] proposed to build a cloud platform based on loT technology to ensure user cases and consultation The privacy situation provides a new paradigm for breaking the traditional medical service; Leligou, Helen C. [8] proposed to use cloud platforms to meet the diverse rescue needs and meet the special needs of the disabled.

In our study, we propose a fuzzy computing method for checking score privacy, which implements the user privacy protection function based on fog calculation, which can effectively protect the privacy of citizens and reduce the possibility of privacy leakage of the credit system.

2 Applicaion Architecture Design of E-Commerence Platform Interration System Based on Block Chain Theory

To adapt to the development of e-commerce, many brands in the market have established their own points system and platform to attract consumers. After calculating the customers' consumption, the purpose of giving them rebates in the form of points is to develop customers' consumption habits and form a virtuous circle of stable

*15079056912@163. com

profits. Some consumers also agree with this way of getting VIP courtesy. In view of this, we aim to realise the circulation of credits through the transactions on the block chain, to form a perfect e-commerce points system.

2.1 Design of e-commerce points framework from the perspective of block chain

From the perspective of the blockchain perspective, the system is shown in Figure. 1 and mainly has three points. Firstly, consumers can register and log in their accounts on their network nodes, obtain points in the following transaction process, conduct the operations of points query and use, and backup the data of each transaction. Secondly, the e-commerce platform and the brand share different nodes, but have similar functions and highly interoperable information. Thirdly, at the centre of the blockchain system is the multi-party secure computing platform. The operation of this system is based on MPC encryption algorithm.

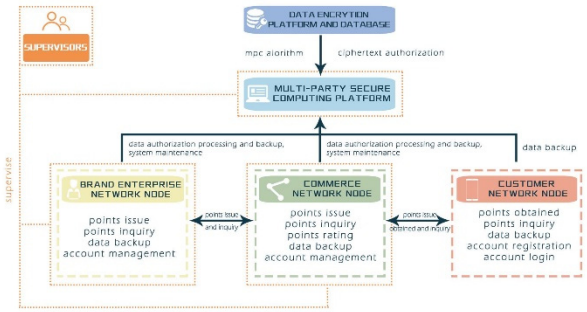

Figure. 1 the framework of the multi-party platforms in the blockchain

2.2 The application architecture of points issuing in the whole system

In a complete application framework (as shown in Figure 2), consumers can efficiently and simply obtain point information and operate points. The core of the system is the computing platform and encryption platform. When the original data of the e-commerce platform and brand customers are connected to the computing system, the data encryption platform will authorise the algorithm and data use. Then the computing party will perform various required calculations on the encrypted original data within the framework of the consensus rules. Finally, the results are directly generated for the entire network broadcast. The platform does not need to know the calculation process, and the calculation side will not know the original calculation data. The entire operation can be supervised by the supervisor, and safety and convenience are guaranteed. In this framework, each node and encryption system perform their duties. And because of the decentralised nature of the blockchain, information cannot be tampered with, and the original data will not be leaked.

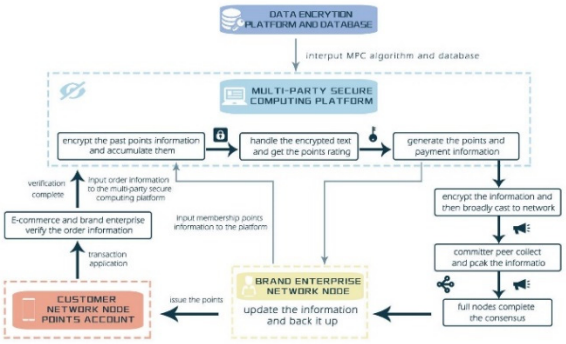

Figure. 2 the flow chart of the points processing

2.3 Case Study

Step 1. Suppose Mallory bought a certain kind of cufflinks from a brand store and gained $2600 points in the brand member account.

Step 2. Mallory selects the cufflinks from the e-commerce platform and applies for the transaction.

Step 3. The order information without customer privacy is submitted through the e-commerce platform and accessed to the multi-party secure computing platform.

Step 4. The data encryption platform connects the algorithm, database and data ciphertext to the multi-party secure computing platform (the data encryption platform authorises the algorithm and data usage of the multi-party secure computing platform).

Step 5. The brand party submitted the previous points information of Mallory's member account and connected it to the multi-party secure computing platform.

Step 6. In the multi-party secure computing platform, the USD 2600 points obtained from the store of the brand and the USD 3200 points obtained from the transaction on the e-commerce platform are encrypted, respectively.

Step 7. Cumulatively calculate the encrypted ciphertext, and compare it with the ciphertext corresponding to 2000, 5000 and 10000.

Step 8. The points information is generated and sent to the brand, which receives the points information.

Step 9. The multi-party secure computing platform encrypts the corresponding payment information and point transaction information obtained by the encryption system, and then broadcasts the entire network. Next the accounting node collects and packages and broadcasts the whole network again.

Step 10. Finally, Mallory's brand membership account updates its membership level, along with data updates and backups. Mallory enjoys a new level of membership.

3 Preliminaries on Order Preserving Algorithm

3.1 Order Preserving Algorithm Based on Homomorphism Cryptosystem

In 2004, the order-preserving encryption algorithm was proposed by Agrawal[2]. However, there is still no solution to the MPC problem in the scenario presented in

this article. For the millionaire problem, Lin et al. [1] proposed an efficient solution, and Zuo et al. Proposed a scheme based on Paillier encryption [4] to optimise it. The algorithm is the order preserving algorithm based on homomorphism cryptosystem

Participant: Alice and Bob; Input/ Output: plaintext (number) x and y / $P(x, y)$

Step 1. (G, D, E) and λ are Paillier Cryptosystem Scheme and security parameter respectively.

Step 2. Alice executes $G(\lambda)$ to get public key and private key and publishes the public key. Alice sends vector encryption $E(A) = (E(a_1), ..., E(a_m))$ to Bob with public key.

Step 3. Bob selects $r_b < N$ randomly and computes

$$E(v) = r_b^N (\prod_{s=1}^{j-1} E(a_s))^2 E(a_j) \bmod N^2$$

Step 4. Alice uses private key to decrypt $E(v)$ and get $x > y, v = 0; x = y, v = 1; x < y, v = 2;$

4 Our Proposed Scheme Based on MPC

4.1 The process of secure multiparty computing

The solution to the millionaire problem put forward by Zuo[5]. In this section, we will propose a collaborative computing scheme on a multi-party secure data platform based on the data flow structure shown in Figure 2. The two parties collaborate to complete the results and processes on a finite set of specified big data.

Participant: Brand enterprise and it' s database, data encryption enterprise and it's database, MPC Platform.

Input: plaintext (number) A and B from brand enterprise and enterprise database respectively. The algorithm from MPC platform.

Output: The results of two party security cooperation calculation.

Initialisation:

Step 1. In the scenario shown in Figure 2, the integer values A , B , $f(A)$, and $f(B)$ are not particularly large in theory. Therefore, the burden of data sets is small, the scheme is based on the data collection in the data set of the two parties, and then sorts the combined operations that they may participate in. Suppose the size of the plain text space of A and B is m and n respectively, the size of the plain text space of f and g of the non-unit multiplicative mapping is k, as well as the size of the space of other interfering data and the data participating as a constant is s. Then the spatial complexity of the data set in this construction process is $((k+1)(n+m)+s)$ and the time complexity is $O(((k+1)(n+m)+s)\log((k+1)(n+m)+s))$.

Step 2. After sorting the data results that may be obtained in the above conditions, the temporary trust institution uses the negotiated all-homomorphic key $(Enc(\cdot), Dec(\cdot))$ to encrypt the data rows of the ordered set, and after the order value is marked beside the ciphertext, the data set is given to the two participants, and the spatial complexity of the data set is $2((k+1)(n+m)+s)$.

Step 3. After the completion of the construction, the two participants only know the plaintext of the two parties and their positions in the whole constructed ordered set, where the process takes the form of $\max(f(Enc(A)), g(Enc(B)))$ compound operation, where A and B are the input of the two parties respectively, and the calculated collaboration function is Max (min(Max (A *0.37, B * 1.5) * 100, 150000),50000). First of all, we will adjust the participation value according to the structure of the regular expression to be F(A, B)= Max (min(Max (A * 37,B * 150), 150,000),50000). Where f(A) is equal to A times 37, and g(B) is equal to B times 150 is an integer. And in the process of calculating f(A) and g(B), we will use the addition operation based on the fast power of multiplication to replace the multiplication homomorphic operation to ensure the efficiency of the operation.

Step 4. In order to ensure that the data is not directly seen in the ciphertext of MPC platform and is directly queried by the other party, the participant's full homomorphic key $(Enc_A(\cdot), Dec_A(\cdot)), (Enc_B(\cdot), Dec_B(\cdot))$ is used to preprocess the data respectively.

4.2 Phase of security collaborative computing

Target: For a more specific example of general term calculation, we perform step decomposition, and we assume that the simplified formula is as follows:

$\max(\min(\max(f(A), g(B)) - C, D), E)$, $Enc(C), Enc(D), Enc(E)$ is a known public integer, and formula to be calculated is $\max_{op3}(\min_{op2}(\max_{op1}(f(Enc(A)), g(Enc(B))) - Enc(C), Enc(D)), Enc(E))$, Where $\max_{opi}(-,-)$ and $\min_{opi}(-,-)$ are the maximum homomorphic functions of this step.

Next, the phase of security collaborative computing is as follows:

Step 1. The query requester initiates the request, and the MPC platform determines the calculation function and accepts the request. The two participants select two symmetric homomorphic keys they know and encrypt the messages as $Enc_A(A)$ and $Enc_B(B)$ into the MPC platform. According to the nature of the exchange order homomorphism all key $Enc(\cdot)$ to calculate the $f(Enc(Enc_A(A)))$ and $g(Enc(Enc_B(B)))$. In addition, the two parties respectively get f (A) and g (B) ready and use the search order of encrypted cryptograph ciphertext data collection to find out $f(Enc(A)) = Dec_A(f(Enc(Enc_A(A))))$ and $f(Enc(B)) = Dec_B(f(Enc(Enc_B(B))))$, respectively corresponding to the order of the values of i and j (including i and j values respectively by their own side know).

According to the properties of the full homomorphic key $Enc(\cdot)$ that can be exchanged with $Enc_A(A)$ and $Enc_B(B)$, the max and min homomorphic functions are calculated by the MPC platform. Also, the two participants respectively calculated the values of f(A) and g(B) logically and used the encrypted ciphertext to find the ordered ciphertext data set, to find out the to correspond sequential values of f(A) and g(B), which were denoted as i and j respectively (where the values of i and j were respectively known by their own party).

Step 2. Base on Algorithm 2, both of parties know the size relationship of f(A) and g(B) without leaking A and B. Then they will tell the MPC platform about the size relationship between the two values. If the results are consistent, go to the next step. If not, repeat this step. This step realises the function of $ans_1 = \max_{op1}(f(Enc(Enc_A(A))), g(Enc(Enc_B(B))))$ .Note that when the numerical value calculated by the participants is the same, only two participants know the data held by the other party, and MPC platform can't know it. At this time, all the data are reported by the brand enterprise.

Step 3. Calculate the value after reading ans_1 and $Enc(C)$, $Enc(D)$. If A (one of the holders of data) wins, they need to perform table lookup calculation $ans_2 = Enc_A(\min_{op2}(Dec_A(ans_1) - Enc(C), Enc(D)))$, equal to compare two numbers (plaintext) and returned to the MPC platform; Then, execute this step again, calculated $ans_3 = Enc_A(\max_{op3}(Dec_A(ans_2), Enc(E)))$ by the brand, the calculated results are returned to the MPC platform.

Step 4. The request port is automatically computed $ans_4 = Dec(Dec_A(ans_3))$ to obtain the desired result.

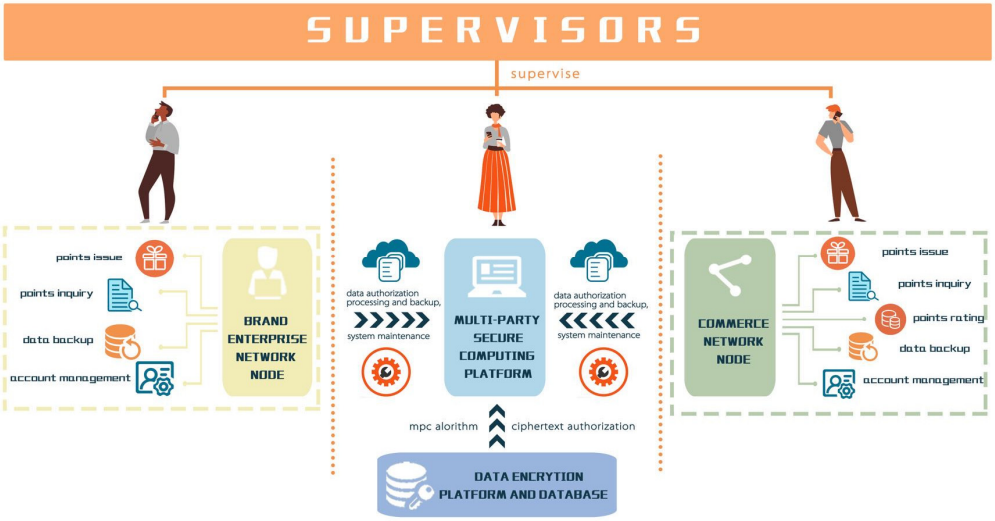

Figure 3. Data flow diagram of multiparty secure computing platform

4.3 Correctness of Our Scheme

The following set of equations can be obtained from the properties in the scheme:

$$\max_{opi}(Enc(A), Enc(B)) = Enc(\max(A, B)); \min_{opi}(Enc(A), Enc(B)) = Enc(\min(A, B));$$

$$\max_{opi}(Enc_A(A), Enc_B(B)) = Enc_A(A), A \geq B; \max_{opi}(Enc_A(A), Enc_B(B)) = Enc_B(B), A < B;$$

$$\min_{opi}(Enc_A(A), Enc_B(B)) = Enc_A(A), A \leq B; \min_{opi}(Enc_A(A), Enc_B(B)) = Enc_B(B), A \leq B;$$

Therefore, the $\max_{opi}(-,-)$ and $\min_{opi}(-,-)$ represent two homomorphic functions in our scheme, so the verification process is as follows:

$$ans_1 = \max_{op1}(f(Enc(Enc_A(A))), g(Enc(Enc_B(B)))) = Enc_A(Enc(\max(f(A), g(B))))$$

$$ans_2 = Enc_A(\min_{op2}(Dec_A(ans_1) - Enc(C), Enc(D))) = Enc_A(\min_{op2}(Enc(\max(f(A) - C, g(B) - C))), Enc(D)))$$

$$ans_3 = Enc_A(\max_{op3}(Dec_A(ans_2), Enc(E)))) = Enc_A(\max_{op3}(\min_{op2}(Enc(\max(f(A) - C, g(B) - C)), Enc(D)), Enc(E))))$$

$$ans_4 = Dec(Dec_A(ans_3)) = \max(\min(\max(f(A), g(B)) - C, D), E)$$

Hence, the correctness of our proposed scheme is verified.

4.4 Security Analysis

We analysed the proposed scheme from the aspects of privacy, integrity, forward security and confidentiality of the message. Order Preserving Algorithm Based on Homomorphism Cryptosystem ensures a plaintext size comparison between the brand side and the data encryption platform side, which can be done without disclosing data privacy to participants other than themselves and third parties. The full homomorphic encryption of authentication ensures the information of the participants is not queried by other participants through ciphertext retrieval. These operations guarantee the privacy of our scheme. At the same time, we guarantee the confidentiality of our scheme under the premise of high efficiency through full homomorphic encryption with less number of operations. In addition, the open 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 full homomorphic keys for different users' queries.

5 Conclusions

Blockchain and multi-party security computing are a group of people interacting according to specific rules

(protocols). The blockchain is mainly to verify the correctness of the completed calculation. This can achieve consistent recognition of the results and prevent tampering of the result records. The blockchain emphasises the verifiability of computing. Multi-party security calculation (MPC) obtains the calculation result under the condition of keeping the input secret. This emphasises the confidentiality of the input data during the calculation process. This article proposes a solution designed for a static network. It is based on small-scale encryption on the same platform and is applied to the calculation scheme on a multi-party secure data platform. This scheme can complete the calculation verification and the confidentiality of the input data at the same time. This application has practical significance for the development of e-commerce systems and traditional brand operations.

The current combination of blockchain technology and multi-party secure computing technology is also being explored. It is difficult to achieve dynamic database comparison problems, resulting in the database cannot be updated in real time. Periodic calculation consumes more costs in a certain sense, resulting in a waste of resources. In order to enhance its convenience and practicality in the application, we will perfect the dynamics of the technology in future research. It is hoped to realize the real-time collaboration, unification of verifiable calculation, confidentiality of input data, and database update.

Acknowledgment

The research is supported by the student research project (No. 2020062115430508) of Jiangxi University of Finance and Economics.

References

1. Hsiao-Ying Lin, Wen-Guey Tzeng. An Efficient Solution to the Millionaires ' Problem Based on Homomorphic Encryption[J].
2. Agrawal, Rakesh, Kiernan, Jerry, Srikant, Ramakrishnan,et al. [ACM Press the 2004 ACM SIGMOD international conference - Paris, France (2004.06.13-2004.06.18)] Proceedings of the 2004 ACM SIGMOD international conference on Management of data, - SIGMOD \"04 - Order preserving encryption for numeric data[J]. :563.
3. Sergey Krendelev, Mikhail Yakovlev, Maria Usoltseva. Secure Database Using Order-Preserving Encryption Scheme Based on Arithmetic Coding and Noise Function[C]// Information and Communication Technology - EurAsia Conference. Springer International Publishing, 2015.
4. Pascal Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes[C]// Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding. 1999.
5. Zuo Xiangjian, Li Shundong, Yang Xiaoli. Efficient solution to homomorphic encryption millionaire problem [J]. Minicomputer system, 2017 (3).
6. Esposito, C (Esposito, Christian); Castiglione, A (Castiglione, Aniello); Tudorica, CA (Tudorica, Constantin-Alexandru); Pop, F (Pop, Florin)//Security and Privacy for Cloud-Based Data Management in the Health Network Service Chain: A Microservice Approach.2017.
7. Kaw, JA (Kaw, Javaid A.); Loan, NA (Loan, Nazir A.) ; Parah, SA (Parah, Shabir A.); Muhammad, K (Muhammad, K.); Sheikh, JA (Sheikh, Javaid A.)//A reversible and secure patient information hiding system for IoT driven e-health10.1016/j.ijinfomgt.2018.09.008,2018.
8. Leligou, HC (Leligou, Helen C.); Panagiotis, A (Panagiotis, Athanasoulis); Tsakou, G (Tsakou, Gianna) ; Vanderheiden, G (Vanderheiden, Gregg); Touliou, K (Touliou, Katerina); Kocsis, O (Kocsis, Otilia) ; Katevas, N (Katevas, Nikos)//Generic platform for registration and online offering of assistance-on-demand (AoD) services in an inclusive infrastructure. 2019.
9. Piao, CH (Piao, Chunhui); Shi, YJ (Shi, Yajuan) ; Yan, JQ (Yan, Jiaqi) ; Zhang, CY (Zhang, Changyou); Liu, LP (Liu, Liping)// Privacy-preserving governmental data publishing: A fog-computing-based differential privacy approach //Future generation computer systems-the international journal of science.JAN 2019.