International Journal of Smart Business and Technology
Vol.8, No.1 (2020), pp.1-12
http://dx.doi.org/10.21742/ijsbt.2020.8.1.01

Personal Credit Information Privacy Protection based on Homomorphic Encryption Algorithm

Nazlie Shahmir[1] and Nasim Muhammad2

[1,2]*School of Information Technology, Deakin University, Geelong, Australia*
[1]*nazlie.shahmir@deakin.edu.au*, [2]*nasim.muhammad@deakin.edu.au*

Abstract

With the continuous development of information technology, the construction of digital government is also accelerating. In the construction of digital government, smart contracts and homomorphic encryption technology of blockchain are combined. Based on the smart contract technology of the blockchain, this paper proposes a personal credit reporting privacy protection plan, which specifically includes the credit reporting system model and smart contract design. At the same time, it analyzes the specific operations such as adding access nodes and setting node permissions involved in this project. Through multi-party protection of personal privacy of credit investigation, automatic matching of user conditions for credit investigation access is realized. Since the solution in this article involves many contracts, we will further optimize the overall operating efficiency of the solution by strengthening the privacy protection during the message transfer process and improving the execution efficiency of the homomorphic encryption algorithm.

Keywords: *Blockchain, Smart contract, Paillier homomorphic encryption algorithm, Personal credit information, Privacy protection*

1. Introduction

With the continuous development of information technology, the construction of digital government has made significant progress, and it is moving rapidly in the direction of intelligence and platform. In recent years, the construction of a social credit system has become a trend. By accelerating the construction of a credit-centric social credit evaluation system, promoting government digital office work, and creating a good credit environment. In the process of government digital transformation, it is necessary to form data sharing, integrate cross-departmental and cross-regional data to establish a sound social credit system [1], but there are personal privacy leaks in the construction of the social credit system, so the privacy of personal information protection is an urgent problem to be solved [2].

In recent years, blockchain technology has developed rapidly. Because it uses a variety of core cryptography technologies, such as elliptic curve encryption algorithm, anti-quantum encryption algorithm [3], etc., it has the characteristics of relative security and decentralization, so it is applied There are more and more researches on privacy protection [4][5][6]. Literature [7][8] proposes to apply blockchain technology to the personal credit investigation system. Literature [9] proposes to combine blockchain and big data to build a credit system and overcome the shortcomings of the traditional credit system by integrating various local data. Literature [10] applies blockchain technology to the field of intellectual property protection and

Article history:
Received (December 1, 2019), Review Result (January 5, 2020), Accepted (March 10, 2020)

Print ISSN: 2288-8969, eISSN: 2207-516X IJSBT

proposes an intellectual property privacy protection model using the blockchain consensus mechanism. Literature [11] applies blockchain technology to the privacy of electronic health records and proposes a privacy protection plan for electronic health records. Literature [12] applies blockchain technology to medical data to realize data sharing among medical institutions. However, since the construction of digital government is still in its infancy, and the construction of the social credit system has not been put into use during the preparatory process, there are relatively little researches on the protection of personal credit information privacy in the construction of the social credit system, and the blockchain technology The research applied to the field of personal credit privacy protection has very high research value and practicality.

2. Basic theory

2.1. Blockchain technology

Blockchain originated from Bitcoin [13][14], which is a distributed ledger (database) technology that organizes and processes data messages in the form of blocks in chronological order and cryptographically guarantees that the data cannot be tampered with or forged. The main underlying technologies of the blockchain include cryptography-related technologies, consensus mechanisms, smart contracts, distributed storage, etc. Blockchain technology is the product of the combination of a variety of computer technologies. It is essentially a decentralized distributed ledger database technology that sequentially combines data blocks into a chain data structure through a peer-to-peer network Shared data ledger, the bottom layer is a series of related data blocks generated by cryptographic methods. All participating nodes jointly maintain the blockchain, where each node regularly exchanges information with neighboring nodes to ensure the synchronization of global ledger information. Therefore, blockchain technology has the characteristics of decentralization, de-trust, transparent rules, collective maintenance, and non-tampering [15]. To prevent the private data of each node from being stolen, blockchain technology uses data signature algorithms to protect privacy, such as elliptic curve signature algorithms, anti-quantum cryptographic algorithms, ring signature algorithms, etc.

Blockchain technology uses a consensus mechanism to ensure that each node has a unique and recognized global ledger [16]. The consensus mechanism is mainly responsible for selecting and verifying related nodes. The consensus mechanism guarantees the decentralization of blockchain trust establishment. Common consensus mechanisms include Proof of Work [17][18], Proof of Stake [19][20][21], Proof of Space [22], Proof of Luck [23], Proof of Elapsed Time [24], Delegated Proof of Stake [25], Proof of Useful Work [26], alliance chain Quorum [27], etc. The scheme in this paper uses the Quorum consensus algorithm of the alliance chain in the consensus mechanism of blockchain technology to establish a trust scheme. The algorithm is based on a voting mechanism, which stipulates that some nodes have voting rights, and require nodes to reach a certain amount of voting before they can be added to the blockchain.

Ethereum is a decentralized application platform that can execute smart contracts. The EVM (Environment Virtual Machine) is the operating environment of smart contracts in Ethereum, supporting complex logic control, and its essence is a transaction message transfer system. In the process of smart contract invocation, since each node will conduct information transactions, all nodes will pay a huge contract execution cost for information transactions. The cost is counted in gas as the unit, and the upper limit is the gas limit. Only when the total consumption is less than the gas limits. The transaction will be executed at the time, otherwise, the transaction will fail.

At present, the industry does not have a unified definition of smart contracts. BUTTERIN [28] pointed out that smart contracts are a set of commitments defined in digital form, including agreements on which contract participants can execute these commitments. Ethereum's smart contracts are based on blocks. Digital information program supported by chain technology. SZABO [29] pointed out that a smart contract is a computer transaction agreement that can execute contract terms. Because the essence of a smart contract is program code, which involves some algorithms and business logic, it programmatically programs the complex relationships in the actual application process. The automatic execution can be realized by putting it into use, and blockchain technology provides the necessary conditions for the realization of smart contracts [30].

2.2. Cryptography

Homomorphic encryption is an encryption transformation technology that allows direct manipulation of ciphertext [31]. For example, two ciphertexts $M(x)$ and $M(y)$ satisfy the calculation formula of $M(x)\otimes M(y) = M(x\otimes y)$, which means addition, subtraction, multiplication, and division operations, so they will meet the requirements of addition, subtraction, multiplication, and division at the same time. Homomorphic operation is called fully homomorphic encryption.

PAILLIER proposed a probabilistic public-key encryption system in 1999, called Paillier encryption [32]. Paillier encryption is a homomorphic encryption algorithm, which is based on the difficult problem of compound residual classes and satisfies the homomorphism of addition and multiplication. The specific process of the algorithm is as follows:

Generate a key, randomly generate two large prime numbers p and q， need to meet gcd $(pq, (p-1)(q-1)) = 1$。 Calculation n = pq，λ = lcm $(p-1, q-1)$， pick any integerg $\in Z_{n^2}^*$， make μ $= (L(g^\lambda mod n^2))^{-1}$， where $L(x) = \frac{x-1}{n}$。 So far, public key (n, g) and private key (λ, μ) are generated.

Encrypt the plaintext m, select a random integerr $\in Z_{n^2}^*$, $0 < r < n$， Satisfy$gcd(r， n) = 1$， The ciphertext is$c = E(m， r) = g^m \cdot r^n mod\, n^2\ (0 < m < n)$。

The receiver decrypts the received ciphertext c and calculates $m = D(c) = L(c^\lambda mod\, n^2) \cdot \mu mod\, n$ get the plaintext.

3. Personal credit privacy protection plan

This section introduces the personal credit reporting privacy protection scheme based on blockchain smart contracts, including the credit reporting system model and smart contracts. It also introduces specific operations such as adding access nodes, setting node permissions, and condition matching involved in the scheme in this article.

3.1. Credit information system model

The credit investigation system model in this paper is shown in [Figure 1], which mainly includes credit investigation individuals, blockchain credit investigation system, credit investigation visitor users, and credit investigation information providers.

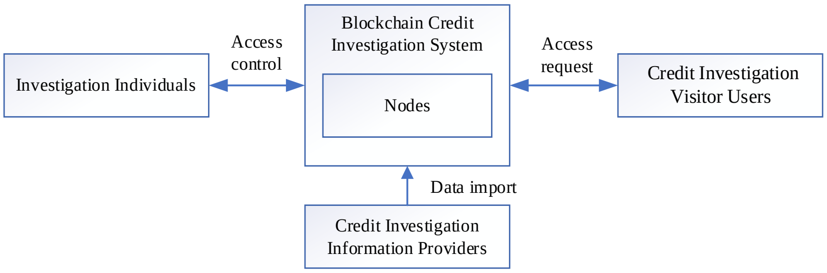
Investigation Individuals
Access control
Blockchain Credit Investigation System
Nodes
Access request
Credit Investigation Visitor Users
Data import
Credit Investigation Information Providers

Figure 1. Model of the credit system

(1) Credit reference individual

In the process of building the social credit system, the credit information of five types of entities: enterprises, natural persons, social public institutions, and government agencies has been collected. Credit files have been established and data characteristics have been collected to carry out public credit evaluation. These five types of subjects are called credit individuals. Credit reporting individuals can view their credit reporting information through smart contracts. For some of the information that meets the authority, the credit reporting individual can change the access rights of other users to this information, to realize the access control rights of the credit reporting individual to their credit reporting information.

(2) Blockchain credit investigation system

A complete social credit system, in addition to individual credit reporting, should also include a credit reporting platform, which is a system that integrates data in the social credit system. Blockchain technology is used here for data integration. The voting node is the internal credit reporting system. The node is used to verify the legitimacy of the node.

(3) Credit information provider

In the process of integrating the data of all parties, the providers of these data are called credit information providers, which mainly include three types of entities: public institutions, social organizations, and government agencies. Here, credit information providers are not a specific one. Nodes are a group of nodes that need to be connected to various departments of the government credit investigation system, such as traffic violation information provided by the traffic control department, personal credit information provided by the banking system, personal communication information provided by the communication department, and personal taxation provided by the taxation department. Information, personal information provided by the public security system, etc. The credit information provider provides personal credit information to the credit information system.

(3) Credit access users

Credit reporting users refer to subjects who need to inquire about personal credit reporting information through the credit reporting system for some reason. Credit reporting users include the same five types of subjects as credit reporting individuals.

In the credit investigation system model, all personal credit investigation information is stored in the database of the credit investigation system. The credit investigation system will store the symmetric encryption key and part of the credit investigation individual information in the blockchain for access. Individuals can obtain access rights to credit information through the smart contract technology of the blockchain, and use smart contract technology to obtain the encryption key to decrypt the credit information. Voting nodes use the Quorum algorithm of the alliance chain to determine the legitimacy of the new node.

The government completes the collection of data during the construction of the credit information system, and the credit information provider integrates the data into the blockchain credit information system through the data interface. People often use credit information system data in their lives. For example, user A needs to apply to bank B for a loan. At this time, bank B only needs to query the credit information system for user A's credit information to determine whether to approve the transaction. loan application. In this process, user A is the credit reporting individual, and bank B is the credit reporting visitor.

3.2. Blockchain Smart contract

The smart contracts involved in the solution in this article mainly have functions such as consensus judgment, node classification, historical information recording, ownership judgment, permission setting, and condition matching. The details are as follows:

(1) Consensus judgment contract.

The consensus judgment contract contains the Ethereum address of the voting node, which uses the alliance chain Quorum algorithm for consensus judgment. A quorum algorithm is an algorithm that votes on nodes on the blockchain to determine legitimacy. Once a new node is found to join, the voting node will verify the legitimacy of the registered node. Therefore, this function can reduce malicious registration attacks and effectively avoid repeated registrations.

(2) Node classification contract.

The node classification contract contains the category information of all nodes. In the scheme of this article, the node types include three types of credit reporters, credit reporting systems, and credit access users. Therefore, consensus contracts can verify the legitimacy of nodes, while classification contracts can distinguish node types. The contract contains the type flag and the node Ethereum address.

(3) Historical information recording contract.

The historical information record contract contains other node information related to the node, as well as the address of the ownership contract.

(4) Ownership judgment contract.

The ownership judgment contract stores the identity information and credit information of the credit investigation individual, and at the same time stores the address of the authority contract. The ownership contract can track the credit information in the credit information system, and it can also establish data integrity mapping by querying the chain and the hash value of the credit individual.

(5) Permission setting contract.

The authority setting contract stores information related to node authority and the relevant authority is defined according to the node type and specific information. The plan in this article combines the credit investigation system with actual usage and divides 4 levels of authority:

(a) Reading authority, the credit investigation individual, and the credit investigation system have the authority to read personal credit investigation information.

(b) Ownership authority, the credit investigation individual, and the credit investigation system have the ownership authority of the individual credit investigation information, which is the highest level of authority.

(c) Write permission, the credit information provider has the right to write credit information.

(d) Blind reading permission, credit information access users can only read the ciphertext of personal credit information.

(e) Condition matching contract. The condition matching contract contains part of the credit information of the individual credit reference and the condition table of the credit reference visit user and can realize the automatic condition matching function according to the condition table. Among them, the personal information of the credit reference includes the Ethereum address, the calculation result of the condition matching, the hash value of the credit reference message, and the encrypted personal information of the credit reference, etc.

The function of this smart contract is similar to that of a credit reporter applying to the bank for a loan. The bank needs to review the conditions of the loan user. At this time, the bank is the credit visitor, and the bank matches the calculation result in the contract through the access conditions and sends it to the condition matching contract. If the conditions are met, the bank will get the result of successful condition matching and approve the loan application; if the conditions are not met, the application will be rejected. Here, the bank cannot know the specific and clear text information of the applicant's credit investigation.

3.3. Credit information visit user added

The specific steps for adding a credit visit user are as follows:

(1) The credit reference visitor requests the credit reference individual and sends his Ethereum address to the credit reference individual at the same time.

(2) The individual credit reporter approves the request and sends the Ethereum address to the node classification contract.

(3) The node classification contract looks up the address in the database. If it already exists and the category is the same, the operation is complete; otherwise, the node classification contract sends the address to the consensus judgment contract, and the consensus judgment contract will vote for verification.

(4) If the voting verification is successful, the addition of the access node is completed, otherwise, the addition fails.

3.4. Credit information access user permission settings

To protect the privacy of credit information of individuals, users of credit information access cannot obtain the plaintext of credit information of individuals, and can only have the authority to read the ciphertext of credit information, that is, blind authority. Under normal circumstances, the individual credit reporter has the ownership of the credit information, and any form of authority authorization requires the consent of the individual credit reporter. The authorization process is shown in [Figure 2]. The specific steps are as follows:

(1) The credit reference visit user first initiates an authorization request to the credit reference individual.

(2) After receiving the application, the credit reporter queries the historical information record contract for the authority to access the node.

(3) The historical information recording contract sends the ownership judgment contract information to the credit reporter.

(5) The credit individual applies to the ownership judgment contract for permission to set the contract address.

(6) The ownership judgment contract sends the permission setting contract address to the credit reporter.

(7) The credit reporter initiates a permission change request to the permission setting contract.

The permission setting contract first queries the node information after receiving the permit modification request: if the node information does not exist, save the relevant information of the credit access user in the contract, including the address and permissions; if the node already exists, then compare whether the permissions are the same as the requested permissions, and the permissions are different to update the permissions, otherwise no operation is required. The applicant for changing the authority can be the credit investigation system, but for some credit investigation information, the credit investigation system needs to first ask the credit investigation individual's wishes before changing the credit investigation access user authority.

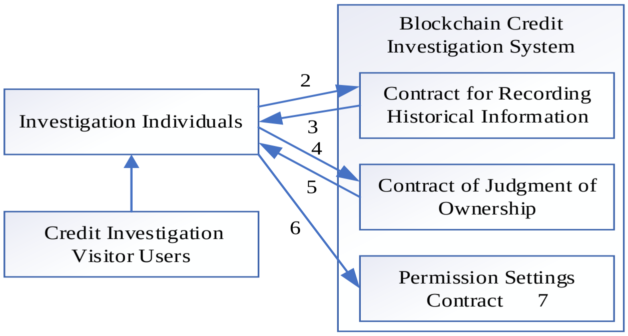
Blockchain Credit Investigation System
Investigation Individuals
Contract for Recording Historical Information
Contract of Judgment of Ownership
Permission Settings Contract
Credit Investigation Visitor Users
2
3
4
5
6
7

Figure 2. Process of authorization

3.5. Credit information access user conditions match

To solve the problem of the traditional credit information verification process that the credit information visitor needs to view the plaintext of the credit information of the individual credit information, this paper proposes a blockchain-based automatic condition matching scheme. The scheme uses the Paillier homomorphic encryption algorithm to make the credit-visiting user hold the key pair. In this scheme, the credit reference visitor will create a special credit reference condition application form based on the individual credit reference application. To ensure that the contract information cannot be tampered with, the credit reference condition application form cannot be changed once it is created. If you want to call the conditions to match the contract, you need to know the contract address.

In the condition matching process, the credit information visitor only interacts with the credit information system and the condition matching contract. The following is an example of an application by a credit investigation individual to the bank to explain the condition matching process, where the credit investigation individual is the loan applicant and the bank is the credit visit user, and it is assumed that the government credit investigation platform has been constructed, and the credit investigation information of all individual users It has been summarized in the credit investigation system, and the specific matching steps are as follows:

(1) The loan applicant submits a loan application to the bank, and the bank generates a loan application condition form based on the loan amount applied by the applicant.

(2) The bank submits a request for access to personal credit information to the credit information system.

(3) The credit reporting system confirms the bank access authority to the credit reporting individual, and after obtaining the authorization of the credit reporting individual, the credit reporting system responds to the request.

(4) The bank encrypts the loan application condition form into ciphertext $E(M_1), E(M_2), \cdots, E(M_n)$, and then sends the ciphertext to the credit investigation system.

(5) The credit reporting system creates a condition matching contract and calculates the hash value of the credit information encrypted by the symmetric encryption key through $E(M_1) \times E(M)^{-1}, E(M_2) \times E(M)^{-1}, \cdots, E(M_n) \times E(M)^{-1}$ Calculate the ciphertext matching result, and put the result into the array $A[n]$ out of order, and put the individual's Ethereum address, The calculated hash value and the array $A[n]$ are stored in the condition matching contract.

When the condition matching contract is established, the bank accesses the condition matching contract to obtain the calculation results in the array $A[n]$ and uses the private key to decrypt it. If the decryption result is 0, it means that the two plaintexts are the same and meet the loan conditions, and the loan application is agreed upon. Otherwise, it means that the loan applicant does not meet the loan conditions and the loan application is rejected. Since the calculation results are stored in the array $A[n]$ out of order, the bank cannot know which conditions are matched and mismatched, which protects the privacy of credit information of individuals.

4. Solution performance analysis

4.1. Correctness analysis

After the credit visit user obtains the array $A[n]$ from the condition matching contract, the private key can be used to decrypt the data in the array to verify the correctness of the data.

Since the homomorphic encryption algorithm is used in the solution in this article, the credit visitor can decrypt successfully using the private key. The specific proof process is as follows: $E(M) \times E(M_1) = (g^m \times r^{n_1}) \times (g^{m_1} \times r^{m_2})^{-1} mod\, n^2 = (g^{m-m_1} \times g^{n_1-n_2})n^2 = E(M - M_1)$. Therefore, if$M = M_1$，则$D(E(M) \times E(M_1)^{-1}) = D(M - M_1) = 0$，thereby verifying the correctness of the scheme in this paper.

4.2. Safety analysis

Since the credit reference visitor cannot know the credit information on the credit reference personal condition form, the reason is that the credit reference system sends back to the credit reference visitor out of order the calculation results accessed by the credit reference visitor. If you want to get the clear text It is very difficult, and the result is stored in the array $A[n]$ out of order, even if the probability of obtaining the plaintext is only 1/n (n is the number of credit information on the credit application form), so the security of this solution is very high.

4.3. Anonymity analysis

Since the Paillier encryption algorithm is secure, if there is no private key, it is impossible to obtain any piece of plaintext information about M_i from $E(M_i)$. Otherwise, the solvable difficult problem of the composite remainder will contradict it, so the credit information system cannot Use $E(M_1), E(M_2), \cdots, E(M_n)$ to infer the plaintext information M_1, $M_2 \cdots$, M_n in the condition application form set by the credit visit user.

4.4. Privacy protection analysis

In the scheme of this article, the credit information of the individual credit information is only known by the storage party, and all the plaintext messages in the credit information system cannot be known by any other party. For the credit information that the credit reporter has no authority, the credit reporter cannot know it. For credit reference users, only have access rights if the credit reference individual agrees and authorizes. In the process of accessing the corresponding credit information, only a comparison results of the credit reference information corresponding to the credit reference information can be obtained. Know the specific credit information, so the privacy of the credit information of the individual is protected. In addition, the credit information system cannot infer the content of the credit information inquired by the credit user through the access application form of the credit user, nor can it know the purpose of the credit information individual for inquiring about the credit information, thus protecting the information. Believe in personal privacy. In summary, the solution in this paper can protect the privacy of credit information of individuals from multiple perspectives.

4.5. Operating cost analysis

When establishing an automatic condition matching contract, the main operation outside the blockchain is the application of credit information access users. The credit information platform uses homomorphic encryption calculations, and its operating cost is low. The operations on the blockchain are mainly contracted data storage and retrieval, and the contract execution cost of data gas is determined by the size of the data operated, and the cost is less than half of the gas limit. Therefore, the contract transaction can be executed, which verifies that the solution in this paper has a relatively high performance. Low operating costs.

5. Conclusion

Based on the smart contract technology of the blockchain, this paper proposes a personal credit reporting privacy protection plan, which specifically includes the credit reporting system model and smart contract design. At the same time, it analyzes the specific operations such as adding access nodes and setting node permissions involved in this project. Through multi-party protection of personal privacy of credit investigation, automatic matching of user conditions for credit investigation access is realized. Since the solution in this article involves many contracts, we will further optimize the overall operating efficiency of the solution by strengthening the privacy protection during the message transfer process and improving the execution efficiency of the homomorphic encryption algorithm.

References

[1] N. Loubere and S. Brehm "China's dystopian social credit system is a harbinger of the global age of the algorithm," **(2018)**

[2] H. Abdullah "A structural and navigational method for integrated organizational information privacy protection," pp. 1-9, **(2018)**

[3] M. Khan and A. Rasheed "Permutation-based special linear transforms with application in the quantum image encryption algorithm," Quantum Information Processing, vol.18, no.10, pp.298, **(2019)**

[4] J. M. Abowd and I. M. Schmutte, “An economic analysis of privacy protection and statistical accuracy as social choices,” Working Papers, **(2018)**

[5] D. Mashima, A. Serikova, and Y. Cheng, “Towards the quantitative evaluation of privacy protection schemes for electricity usage data sharing,” ICT Express, vol.4, no.1, pp.35-41, **(2018)**

[6] J. M. Zeevi, “DNA is different: An exploration of the current inadequacies of genetic privacy protection in recreational DNA databases,” St. John's Law Review, pp.93, **(2019)**

[7] F. Hawlitschek, B. Notheisen, and T. Teubner, “The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy,” Electronic Commerce Research and Applications, pp.29, **(2018)**

[8] P. Vasant, I. Zelinka, and G. W. Weber, “Blockchain technology in the smart city: A new opportunity for smart environment and smart mobility,” Advances in Intelligent Systems and Computing, Intelligent Computing and Optimization, vol.866, no.36, pp.346-354, **(2019)** DOI: 10.1007/978-3-030-00979-3

[9] V. Shaherov, “Features of the formation of the soviet credit system in Irkutsk province during the period of new economic policy,” **(2019)**

[10] Z. Oleksii, S. Zorya, and I. Salohub, “The necessity and importance of state regulation of credit system in agricultural production,” Black Sea Economic Studies, no.48, (2019)

[11] D. K. Boyle, M. Baernholdt, and J. M. Adams, “Improve nurses' well-being and joy in work: Implement true interprofessional teams and address electronic health record usability issues,” Nursing Outlook, vol.67, no.6, pp.791-797. **(2019)**

[12] L. Harrington, “Electronic health record-related events in medical malpractice claims: User error versus use error,” Journal of Patient Safety, pp.15, **(2019)**

[13] S. Billah, “SoK: Research perspectives and challenges for bitcoin and cryptocurrencies,” IEEE Computer Society, **(2015)**

[14] B. Scheuermann and F. Tschorsch, “Bitcoin and beyond: A technical survey on decentralized digital currencies,” Communications Surveys and Tutorials, **(2016)**

[15] R. Pass, L. Seeman, and A. Shelat, “Analysis of the blockchain protocol in asynchronous networks,” Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, Berlin, Germany: Springer, pp.643-673, **(2017)**

[16] I. Bentov, C. Lee, and A. Mizrahi, “Proof of activity: Extending bitcoin’s proof of work via proof of stake,” ACM SIGMETRICS, Performance Evaluation Review, vol.42, no.3, pp.452-458, **(2014)**

[17] C. Badertscher, P. Gazi, and A. Kiayias, “Ouroboros genesis: composable proof-of-stake blockchains with dynamic availability,” Proceedings of 2018 ACMSIGSAC Conference on Computer and Communications Security. New York, USA: ACM Press, pp.913-930, **(2018)**

[18] T. Duong, L. Fan, and H. S. Zhou, “2-hop blockchain: Combining proof-of-work and proof-of-stake securely,” [2019-12-11], https: / /eprint. Iacr. Org /2016 /716

[19] A. Kiayias, A. Russel, and B. David, “Ouroboros: A provably secure proof-of-stake blockchain protocol,” Proceedings of Annual International Cryptology Conference, Berlin, Germany: Springer, pp.357-388, **(2017)**

[20] A. Chepurnoy, T. Duong, and L. Fan, “Twin’s coin: A cryptocurrency via proof-of-work and proof-of-stake [EB /OL], [2019-12-11], https: / /www. Chain news. Com /zh-hant /papers /158251978824. Htm

[21] S. Dziembowski, S. Faust, and V. Lolmogorov, “Proofs of space,” Proceedings of Annual Cryptology Conference. Berlin, Germany: Springer, pp.585-605, **(2015)**

[22] M. Milutinovic, W. He, and H. Wu, “Proof of luck: An efficient blockchain consensus protocol,” Proceedings of the 1st Workshop on System Software for Trusted Execution, New York, USA: ACM Press, pp.2-12, **(2016)**

[23] L. Chen, L. Xu, and N. Shan, “On security analysis of proof-of-elapsed-time (POET),” Proceedings of International Symposium on Stabilization, Safety, and Security of Distributed Systems. Berlin, Germany: Springer, pp.282- 297, **(2017)**

[24] D. Larimer, “Delegated proof-of-stake (DPOS) whitepaper,” [EB /OL], [2019-12-11], https://bit shares talk, Org /index. Php? Topic = 4009. 60

[25] F. Zhang, I. Eyal, and R. Escriva, "REM: Resource-efficient mining for blockchains," Proceedings of the 26th USENIX Security Symposium, Vancouver, Canada; USENIX, pp.1427-1444, **(2017)**

[26] T. Lobban, "Quorum chain consensus," [EB /OL], [2019-12-11], https://github.Com/jpmorganchase/quorum/wiki/QuoQuorumCh-Consensus

[27] V. Buterin, "A next-generation smart contract and decentralized application platform," [EB/OL], [2019-12-11]. https://www.Mendeley.Com/catalog/nextgeneration-smartcontract-decentralized-application-platform/

[28] N. Szabo, "Formalizing and securing relationships on public networks [EB/OL], [2019-12-11], http://www.First monday.org/ojs/index.Php/fm/article/view/548/469

[29] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol.21, no.2, pp.120-126, **(1978)**

[30] P. Paillier, "Public-key cryptosystems based on composite degree residuality classes," Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Berlin, Germany: Springer, pp.223-238, **(1999)**

This page is empty by intention.