Research on Secure Payment in the Process of Currency Transactions in Digital Economy Through Blockchain Technology

Pranjali Deshmukh[1], Nishant Narawade[2], Sanika Mulay[3], Narayan Bhojne[4], Aniket Shelar[5]
[1]*Associate Professor, Department of Computer Engineering, Marathwada Mitra Mandal's Institute of Technology, Lohegaon, Pune, Maharashtra, India.*
[2,3,4,5]*Students, Department of Computer Engineering, Marathwada Mitra Mandal's Institute of Technology, Lohegaon, Pune, Maharashtra, India.*

***Abstract*—This paper briefly introduces the consensus algorithm in blockchain technology. In order to improve the efficiency and security of the consensus algorithm, on the basis of simplifying the consensus steps, the credit mechanism was introduced, and the improved algorithm was applied to the secure payment of digital economy currency transactions. Simulation experiments were conducted. The experiment tested the average response time and throughput of secure payment under different numbers of currency transaction items and different blockchain consensus algorithms. Moreover, the tampering status of transaction information under different numbers of tampered virtual nodes was also tested. The results showed that the average response time of secure payment under the improved practical byzantine fault tolerance consensus algorithm adopted in the currency transaction process was the most stable and shortest. It also had the largest throughput and could effectively resist attacks from third parties.**

***Index Terms*—Blockchain; Currency Transaction; Digital Economy; Secure Payment**

I. INTRODUCTION

Digital economy currency has the characteristics of decentralization, cross-border transactions, and anonymity [30]. With the above characteristics, it has advantages in transaction costs, efficiency, and security [26]. However, with the popularity of digital economy, security problems in the transaction process have gradually emerged, such as transaction information tampering and transaction identity theft [25]. In the digital economy, the issue of secure payment of currency transactions is particularly critical [12,20,23].

Traditional payment systems are confronted with challenges such as cumbersome auditing, high compliance costs, and increased risk of fraud when handling massive transactions [3,10]. These problems not only limit the efficiency of transactions but also threaten the security of users' funds and the business reputation of enterprises [15]. In this context, the emergence of blockchain technology has opened up a new path for secure payment of currency transactions in the digital economy [13,29]. When applied to digital economy currency transactions, blockchain technology can provide digital economy currency transactions with advantages such as efficient payment, transaction transparency, real-time settlement, and smart contracts by taking advantage of its characteristics [7,27].

Mohamed [21] proposed a secure mobile payment framework based on blockchain technology and discussed the advantages of blockchain technology and how blockchain technology provides multi-level authentication to protect mobile-based financial transactions. Jabbar et al.

[14] proposed a blockchain-based solution for establishing secure payment and communication and found through tests that the developed solution was faster and more scalable than existing solutions. Lin et al. [18] proposed a new definition of decentralized conditional anonymous payments.

This paper briefly introduces the consensus algorithm in blockchain technology. In order to enhance the

efficiency and security of the consensus algorithm, on the basis of simplifying the consensus steps, a credit mechanism was introduced. The new algorithm was applied to the secure payment of digital economy currency transactions, and then simulation experiments were carried out.

II. CONSENSUS ALGORITHM IN BLOCKCHAIN TECHNOLOGY

2.1. Blockchain Technology

Blockchain technology is a kind of distributed ledger technology, which records and verifies data through the consensus mechanism among network nodes, providing a secure, transparent and immutable data management method [4,19]. This technology was originally proposed as the underlying technology of Bitcoin, but its application potential far exceeds the field of cryptocurrencies and has now expanded to multiple industries including finance [7], supply chain management [2], and healthcare. Blockchain technology has the following core characteristics [1,11].

2.1.1. Instead of relying on a single management center or server, it is maintained by all nodes participating in the network, making the system more robust and reducing the risk of single point of failure.

2.1.2. Once the information is verified and added to the blockchain, it will be permanently stored and cannot be changed or deleted, ensuring the integrity of the data and the transparency of historical transactions.

2.1.3. Blockchain adopts advanced encryption technology to protect data security, including cryptographic principles such as public and private keys, ensuring the security of transactions and user privacy.

2.1.4. All transaction records are open and transparent to every participant in the network, and anyone can view the transaction history on the entire blockchain.

2.1.5. The smart contracts contained in the blockchain serve as a piece of code running in the blockchain, and contract terms can be automatically executed according to pre-set conditions without the participation of intermediaries, thereby improving efficiency and reducing costs.

The working principle of blockchain includes block generation, consensus mechanism, and transaction verification. In block generation, each new block contains a set of verified transaction records and is linked to the previous block through a cryptographic hash function to form a chain. The consensus mechanism is the algorithm adopted when nodes in the blockchain network need to reach an agreement to confirm the validity of a new block. Common consensus algorithms include Proof of Work, Proof of Stake, etc. Transaction verification means that when a new transaction occurs, it will be broadcast to the entire network, and then verified and packaged into a new block by miners or validators.

2.2. Consensus Algorithm

The guarantee of blockchain technology for safe payment in the digital economy currency transaction process is the distributed storage of information and data. Simply put, the information that needs to be stored is uploaded to a node and broadcast to other nodes, and the uploaded data is copied, and the newly added data in the node constitutes the block chain through the time stamp [24]. When uploading data to nodes of the blockchain network, the key is to synchronize the stored information. In order to ensure the fairness of nodes participating in synchronization, all nodes need to follow a unified norm, i.e., a consensus algorithm. Using the consensus algorithm, information synchronization between nodes can be realized under the premise of malicious nodes in the network [22]. In general, the basic principle of consensus algorithm is that when the data is uploaded, the nodes in the blockchain network select the master node through some means, and the master node broadcasts the information to be recorded to other nodes for verification. After the verification is passed, each node records the information to the blockchain. The main difference between different consensus algorithms is the method of selecting the master node.

In this paper, the practical byzantine fault tolerance (PBFT) algorithm is adopted as the consensus algorithm of blockchain [5]. Compared with the above-mentioned consensus algorithms, the PBFT algorithm realizes the state synchronization of normal nodes in the network based on the premise that there are abnormal nodes in the blockchain network. As long as the number of abnormal nodes in the network

does not exceed one-third of the total number of nodes, it can ensure the reliability of synchronous data storage.

The steps of the traditional PBFT algorithm are described below.

2.2.1. The client initiates an uploading request to the master node of the blockchain.

2.2.2. When the master node in the blockchain receives the request for uploading, it verifies the request. After the verification is passed, the transaction content in the request (mostly the accounting information that needs to be stored in this article) is first stored in the local transaction pool. When the content of the local transaction pool accumulates to a certain amount, it is packaged into a block and broadcast together with the generated pre-preparation message to other nodes.

2.2.3. After receiving the pre-preparation message and the block at other nodes, the validity of the message is verified. If the verification fails, the uploading process is stopped, and the result is returned to the client; if the verification is successful, a preparation message is generated and broadcast in the blockchain network.

2.2.4. After other nodes receive 2f+1 preparation messages in the blockchain network, they generate submission information and broadcast it in the blockchain network. Here, f is the maximum number of unreliable nodes in the network that can ensure the security of the blockchain, and 3f + 1 satisfies that it does not exceed the total number of nodes in the network.

2.2.5. When a node receives 2f + 1 submission messages from the blockchain network, the previously received block is added to the local blockchain of the node. Then, a message of successful uploading is returned to the client.

2.2.6. After the client receives 2f + 1 messages of successful uploading, it can confirm that the data has been successfully uploaded.

The advantages of the PBFT algorithm lie in low delay and no need to use computing power for mining, which improves the consensus efficiency. However, the disadvantages is that the cumbersome steps of the consistency protocol bring security risks to the master node [28]. Therefore, the consensus steps of the traditional PBFT algorithm are deleted in this paper, and a trust mechanism is introduced to assist the selection of the master node, so as to improve the efficiency and security. The specific steps are as follows.

1) The node initiates a request.
2) The node verifies the stored information in the request through the smart contract. After the verification is passed, the stored information is signed and stored in the local transaction pool. The request with the signature is then broadcast to other nodes in the blockchain.
3) After receiving the broadcast request, other nodes verify the validity of the information stored in the request according to the signature in the request. If the verification fails, the stored information is abandoned. If the verification passes, the stored information is stored in the local transaction pool.
4) The information in the transaction pool is packaged into blocks. The consensus request is then broadcast by the voted master node in the form of << CONSENSUS REQUEST,v,n,Si,Di > ,Block >, where v is the view serial number of the current node network, n is the serial number of consensus request, Block is the packaged block, Si and Di are the signature and summary of the block, respectively.
5) The consensus request is verified from the node, and the consensus confirmation message is broadcast in the form of < CONSENSUS CONFIRMATION,v,n,Si,Di,i > (i is the serial number of the slave node) after passing [8].
6) When the node receives 2f+1 consensus confirmation messages from other nodes, the consensus is reached, and the block is stored in the blockchain.
7) When a round of block consensus ends or the consensus request verification is abnormal, the node view of the blockchain network needs to be switched to change the master node. The master node can package n blocks in each round of block consensus process. Except for the n-th block that is used to store the election result of the master node, the other blocks store transaction

information. When the consensus of n − 1 blocks in one round of block consensus of the master node is completed, the master node broadcasts the voting request, and the node broadcasts the voting information to other nodes after receiving the request. The information format is < V OTE,p,x,i >, where p is the serial number of the node selected by voting, x is the credit grade of the selected node [17], and i is the serial number of the node voted. After receiving the voting information from other nodes, the votes of each node is calculated:

$$point_i = P_i \times X_i, \quad (1)$$

where $point_i$ is the final number of votes of candidate node i, P_i is the polling number of other nodes for candidate node i, and X_i is the credit coefficient of candidate node i. After the count is complete, the node will broadcast the serial number of the candidate node with the highest $point_i$ as the vote result message to the rest of the nodes. After receiving the 2f + 1 vote result messages, if there are f + 1 messages indicating the serial number of the same candidate node, this node will be the master node of the next round of block consensus.

III. SECURE PAYMENT FOR CURRENCY TRANSACTIONS

Since electronic data is relatively easy to tamper with in digital economy currency transactions, secure payments are crucial. As shown in Figure 1, the specific steps are as follows.

1) In the initial stage, buyer A first sends the public key of his e-wallet to seller B. After receiving the key, B also sends the public key of his e-wallet and the service fee to A.
2) Both A and B use the public keys of the two e-wallets to generate the P2SH address [16], which is used for

capital injection and can only be used when the private key signatures of A and B are provided.

3) A creates the capital injection transaction and the refund transaction and then sends the refund transaction to B. The injection transaction is a payment channel funded by the buyer or both parties. After the channel is established, both parties can continue to recharge into it. The output of the channel is controlled by the P2SH address constructed by A and B.
4) Whether A continues to use the service of B is determined. If it continues to use the service, return to Step 5) to update the saved commitment transaction. If it does not continue to use it, it will enter the next settlement stage.
5) When A stops trading or does not continue trading for a long time, it enters the settlement stage. B signs the last updated and saved commitment transaction with A's signature, and then it is uploaded via the consensus algorithm.

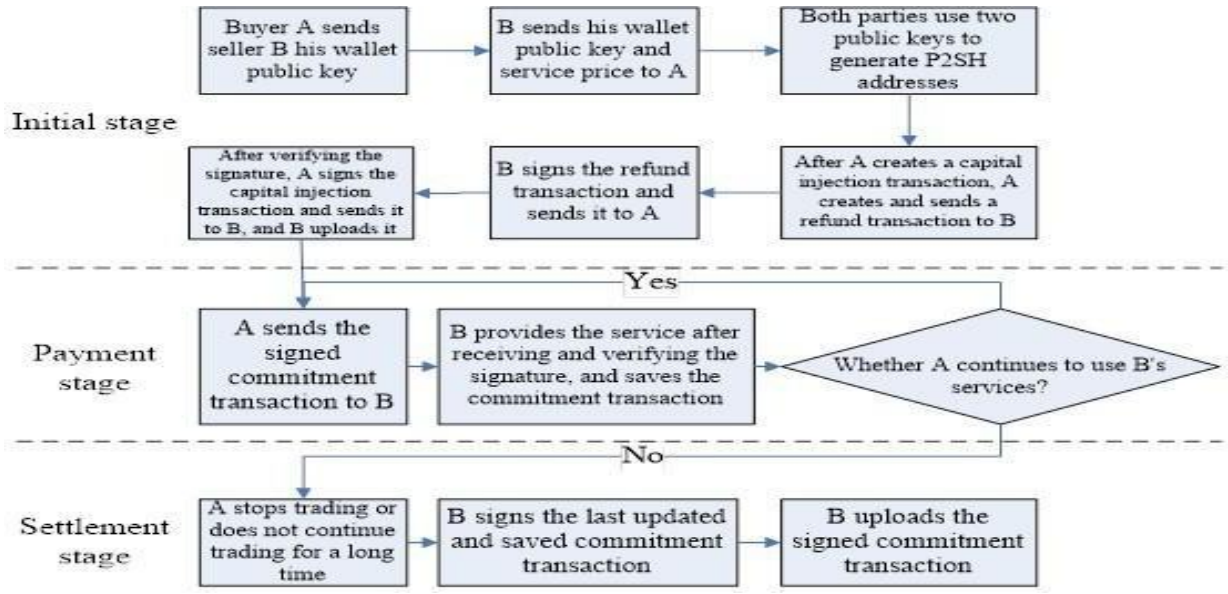

Figure 1: Secure payment process for currency transactions combined with blockchain

The refund transaction is an agreement to withdraw the channel and get their respective funds back when the transaction stops.

6) After receiving the refund transaction, B signs it and sends it to A, A verifies the signature and signs the injection transaction and sends it to B. B uploads the injection transaction with A's signature to the blockchain through the consensus algorithm described above.
7) Entering the payment phase, A generates the commitment transaction, signs it and sends it to B. The commitment transaction is a promise to make payment, and the payment is honored when it is settled after uploading [9].
8) After receiving the commitment transaction, B provides corresponding services for A after verifying that its signature is legitimate and stores the transaction with A's signature.

IV. SIMULATION EXPERIMENT

4.1. Experimental Environment

The simulation experiment was carried out in the server of the laboratory. Server 1 acted as the buyer, server 2 acted as the seller, and server 3 acted as the third-party attacker. The blockchain network nodes were provided by Ethereum. The IP addresses of servers 1 and 2 were stored in the blockchain configuration file during the experiment, and Ethereum provided nine virtual nodes.

4.2. Experimental Setup

1. Blockchain-based secure payment performance test: Server 1 randomly generated 10, 20, 40, 80, and 160 currency transaction items and conducted secure payment simulations with server 2. In the simulation process, the blockchain consensus algorithm was set as proof-of-work (POW), proof-of-stake (POS), PBFT, and the improved PBFT algorithm, respectively, to test the average response time and throughput of secure payment under different numbers of transaction items and different blockchain consensus algorithms.
2. Security test of blockchain-based secure payment: Server 3 tampered with the transaction information stored by the virtual node in the blockchain. Because it was a simulation experiment, it omitted the offensive step and directly made server 3 obtain the number of tampered nodes is shown in Table 3. It can be seen that only when the number of tampered nodes exceeded 5 can the stored transaction information be effectively tampered with. In this simulation experiment, the number of nodes in the blockchain was 11. Suppose the probability of a node failure or successful tampering is 50% (this probability is already very high and should be smaller in actual situations), then at least five nodes need to have problems for the transaction information to change, but the probability that five nodes have problems

Table 1: Average response time of secure payment under different transaction item numbers and consensus algorithms

Consensus algorithm	10 items/ms	20 items/ms	40 items/ms	80 items/ms	160 items/ms
POW	69	91	118	169	198
POS	59	67	79	96	154
PBFT	53	59	66	87	120
Improved PBFT	52	53	55	53	55

Table 2: Throughput of secure payment under different numbers of transaction items and consensus algorithms

Consensus algorithm	10 items/sec	20 items/sec	40 items/sec	80 items/sec	160 items/sec
POW	0.4	0.8	1.6	3.2	6.3
POS	0.6	1.2	2.4	4.8	9.5
PBFT	0.8	1.6	3.2	6.4	12.7
Improved PBFT	1.0	2.0	4.0	8.0	15.8

permission to tamper. After tampering with the transaction information, the transaction information stored in the blockchain platform is queried.

a. Experimental Results

The average response time and throughput of secure payment under different numbers of transaction items and consensus algorithms are shown in Table 1 and Table 2. With the increase of the number of transaction items, the average response time under

the improved PBFT consensus algorithm remained stable and shortest.

As for throughput, with the increase of the number of transaction items, the throughput of each consensus algorithm increased, while under the same number of transaction items, the improved PBFT consensus algorithm always had the highest throughput.

The third-party server was used to tamper with virtual nodes in the blockchain. In the simulation experiment, the attack process was omitted, and the tampering permission was obtained directly. The transaction information queried from the blockchain platform with the increase of

in this experiment was only 3.125%. If the number of nodes in the blockchain was more, the probability would be further reduced. These results revealed that the blockchain could resist tampering attacks.

V. DISCUSSION

Today in the 21st century, with the rapid development of information technology, the digital economy has become an important part of the global economy. Digital currency, as an indispensable part of the digital economy, is gradually changing people's payment habits and financial transaction methods. However, with the rapid growth of digital currency transaction volume, security and privacy protection issues have become increasingly prominent and have become one of the key factors restricting its further development. The traditional payment systems often face many challenges such as data leakage, fraud, and high handling fees. These problems not only affect the trust of users but also pose a threat to the security of the entire economic system. Against this background, blockchain technology, with its characteristics of decentralization, immutability, and high transparency, provides a new solution for solving the problem of secure payment in digital currency transactions.

Since the birth of Bitcoin, blockchain technology has evolved from a simple underlying architecture of cryptocurrency to a revolutionary technology that can be applied in multiple fields. Through distributed ledger technology, it ensures the openness and transparency of all transaction records and uses complex cryptography principles to guarantee the security and integrity of these records. In digital currency transactions, blockchain can not only effectively prevent the problem of double payment, but also greatly reduce human intervention in the transaction process and improve transaction efficiency. Furthermore, the smart contract technology based on blockchain also makes it possible to automatically execute contract terms, thereby enhancing the degree of automation and reliability in the transaction process. Although blockchain has shown great potential in

stored in the blockchain is also tampered with. To achieve this, it is necessary to invade more than five nodes. Even if the success probability of invading one node is amplified to 50%, there is only a 3.125% probability of successfully invading five nodes. Not to mention that in reality, each node has its own firewall and intrusion detection system, leading to a very low probability of a successful invasion. Moreover, as the number of nodes in the blockchain increases, the number of nodes that need to be invaded will also increase, and the probability of successful tampering will be further reduced.

VI. CONCLUSIONS

This paper briefly introduces the consensus algorithm in

Table 3: Tampering status of transaction information under different numbers of tampered virtual nodes

The number of tampered virtual nodes	1	2	3	4	5	6
Whether the queried transaction information has changed	No	No	No	No	Yes	Yes

improving the security of digital currency transactions, its scalability issue is a key point that needs to be urgently addressed, especially in the context of small-amount and high-frequency payments. In this paper, the consensus algorithm in blockchain technology was simplified, and a credit mechanism was introduced to improve security. Then, simulation experiments were conducted to test the impact of the transaction item volume and consensus algorithm type on the efficiency of the blockchain, as well as the security of the blockchain under different numbers of tampered nodes. An increase in the transaction item volume in the blockchain will lead to an increase in throughput, and

the average response time will also change. However, compared with the other consensus algorithms, the blockchain using the improved PBFT consensus algorithm had greater throughput and a smaller and more stable average response time; in terms of security, it effectively resisted tampering attacks from third parties.

The reasons were analyzed. The improved PBFT consensus algorithm has fewer steps compared to the traditional PBFT algorithm. Moreover, a credit mechanism is introduced during the switching and selection of the master node to accelerate the selection. Therefore, the consensus efficiency of the improved PBFT consensus algorithm is greatly enhanced, significantly increasing the throughput of the blockchain and reducing the average response time when processing data. In terms of security, it is a characteristic inherent to the blockchain structure. Under the improved PBFT consensus algorithm, only when more than one-third of the nodes in the blockchain are invaded and tampered with can the tampered information successfully pass the verification of the consensus algorithm and be recorded in the blockchain. In the simulation experiment, 11 nodes were adopted. Therefore, when more than five nodes are tampered with, the data blockchain technology. In order to enhance the efficiency and security of the consensus algorithm, on the basis of simplifying the consensus steps, a credit mechanism is introduced into it and applied to the secure payment of digital economy currency transactions. After that, simulation experiments are carried out. The experiment tested the average response time and throughput of secure payment under the number of different currency transaction items and different blockchain consensus algorithms, and tested the tampering status of transaction information under the number of different tampering virtual nodes. With the increase of the number of transaction items, the average response time under the improved PBFT consensus algorithm remained stable and shortest. As the number of transaction items increased, the throughput under each consensus algorithm increased, and the improved PBFT consensus algorithm had the largest throughput. The number of blockchain nodes in this experiment was 11. When the number of tampered nodes exceeded 5, the stored transaction information was tampered with. Suppose that the probability of the nodes being tampered with was 50%, the probability of the stored transaction information being tampered with in this experiment was only 3.125%.

REFERENCES

[1] T. Alam, “A Survey on The Use of Blockchain for The Internet of Things,” International Journal of Electronics and Information Engineering, vol. 13, no. 3, pp. 119-130, 2021.

[2] P. Y. Chang, M. S. Hwang, C. C. Yang, “A Blockchain-Based Traceable Certification System,” in Security with Intelligent Computing and Big-data Services, Advances in Intelligent Systems and Computing (AISC), vol. 733, Springer, pp 363-369, 2018.

[3] J. Chen, H. Zhang, S. J. H. Wang, “A secure recharge scheme for blockchain payment channels,” Journal of Information Security and Applications, vol. 78, no. Nov., pp. 1.1-1.12, 2023.

[4] L. Chen, Q. Fu, Y. Mu, L. Zeng, F. Rezaeibagha, M. S. Hwang, “Blockchain-based random auditor committee for integrity verification,” Future Generation Computer Systems, vol. 131, pp. 183-193, 2022.

[5] Y. Chen, Z. Chen, D. Hu, “The Reconstruction of Accounting Information Disclosure System Based on Blockchain Technology,” Journal of Physics: Conference Series, vol. 1883, no. 1, pp. 1-5, 2021.

[6] Y. H. Chen, L. C. Huang, I. C. Lin, and M. S. Hwang,“Research on Blockchain Technologies in Bidding Systems,” International Journal of Network Security, vol.22, no. 6, pp. 897-904, 2020.

[7] Y. H. Chen, L. C. Huang, I. C. Lin, and M. S. Hwang, “Research on the Secure Financial Surveillance Blockchain Systems,” International Journal of Network Security, vol. 22, no. 4, pp. 708-716, 2020.

[8] P. Dangayach, “Pharmaceutical supply chain tracking system based on blockchain technology and radio frequency identification tags,” International Journal of Business Research, vol. 19, no. 4, pp. 37-44, 2019.

[9] H. G. Driver, T. Hartley, E. M. Price, A. L. Turinsky, O. J. Buske, M. Osmond, A. K. Ramani, E. Kirby, K. D. Kernohan, M. Couse,

H. Elrick, K. Lu, P. Mashouri, A. Mohan, D. So, C. Conor Klamann, H. G. B. H. Le, A. Herscovich, C. R. Marshall, A. Statia, C. R. C. Consortium, B. M. Knoppers, M. Brudno, K. M. Boycott, "Genomics4RD: An integrated platform to share Canadian deep-phenotype and multiomic data for international rare disease gene discovery," Human Mutation, vol. 43, no. 6, pp. 800-811, 2022.

[10] T. H. Feng, M. S. Hwang, L. W. Syu, "An Authentication Protocol for Lightweight NFC Mobile Sensors Payment," Informatica, vol. 27, no. 4, pp. 723-732,2016.

[11] N. Hamian, M. Bayat, M. R. Alaghband, Z. Hatefi, and S.M. Pournaghi, "Blockchain-based User Reenrollment for Biometric Authentication Systems," International Journal of Electronics and Information Engineering, vol. 14, no. 1, pp. 18-38, 2022.

[12] M. S. Hwang, I. C. Lin, L. H. Li, "A Simple Micropayment Scheme," Journal of Systems and Software, vol. 55, no. 3, pp. 221-229, 2001.

[13] M. S. Hwang and P. C. Sung, "A Study of Micropayment Based on One-way Hash Chain," International Journal of Network Security, vol. 2, no. 2, pp. 81-90, 2006.

[14] R. Jabbar, N. Fetais, M. Kharbeche, M. Krichen, K. Barkaoui, M. Shinoy, "Blockchain for The Internet of Vehicles: How to use Blockchain to secure Vehicle-toEverything (V2X) Communication and Payment?," IEEE Sensors Journal, vol. 21, no. 14, pp. 1580715823,2021.

[15] H. Jiang and L. Liu, "The Weakness of One Blockchain-assisted Authentication and Key Agreement Scheme for Fog-based Smart Grid," International Journal of Electronics and Information Engineering, vol. 16, no. 1, pp. 1-7, 2024.

[16] S. S. Kamble, A. Gunasekaran, M. Goswami, J. Manda, "A systematic perspective on the applications of big data analytics in healthcare management," International Journal of Healthcare Management, vol. 12, no. 3, pp. 226-240, 2019.

[17] L. Koh, A. Dolgui, J. Sarkis, "Blockchain in transport and logistics – paradigms and transitions," International Journal of Production Research, vol. 58, no. 7, pp. 2054-2062, 2020.

[18] C. Lin, D. He, X. Huang, M. K. Khan, K. K. R. Choo, "DCAP: A Secure and Efficient Decentralized Conditional Anonymous Payment System Based on Blockchain," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2440-2452, 2020.

[19] C. Y. Lin, L. C. Huang, Y. H. Chen, and M. S. Hwang, "Research on Security and Performance of Blockchain with Innovation Architecture Technology," International Journal of Network Security, vol.23, no.1, PP.1-8, 2021.

[20] I. C. Lin, M. S. Hwang, C. C. Chang, "The General Pay-Word: A Micro-payment Scheme Based on N-dimension One-way Hash Chain," Designs, Codes and Cryptography, vol. 36, no. 1, pp. 53-67, 2005.

[21] A. O. Y. Mohamed, "Intelligent Blockchain-Based Secure Framework for Transaction in Mobile Electronic Payment System," International Journal of Interactive Mobile Technologies, vol. 17, no. 4, pp. 37-46, 2023.

[22] S. Neupane, A. Baba, F. Wu, F. Yaroh, "Blockchain in accounting: Challenges and future prospects," International Journal of Blockchains and Cryptocurrencies, vol. 2, no. 1, pp. 44-67, 2021.

[23] Z. P. Peng, M. L. Chiang, I. C. Lin, C. C. Yang, and M. S. Hwangh, "CBP2P: Cooperative Electronic Bank Payment Systems Based on Blockchain Technology," Journal of Internet Technology, vol. 23, no. 4, pp. 683-692, 2022.

[24] S. Qiu, "Optimisation of cost accounting method for resource flow based on blockchain technology," International Journal of Information Technology and Management, vol. 21, no. 1, pp. 13-29, 2022.

[25] S. S. Sahoo, M. M. Hosmane, V. Chaurasiya, "A secure payment channel rebalancing model for layer-2 blockchain," Internet of Things, vol. 22, pp. 100822, 2023.

[26] S. F. Tzeng, M. S. Hwang, H. B. Chen, "A Secure On-line Software Transaction Scheme," Computer Standards & Interfaces, vol. 27, no. 3, pp.303312, 2005.

[27] C. C. Wu, C. T. Chang, I. C. Lin, and M. S. Hwang, "Research on Blockchain Secret Key Sharing and Its Digital Asset Applications," International Journal of Network Security, vol. 26, no. 1, pp. 160-166, 2024.

[28] Y. Zhang, F. Xiong, Y. Xie, X. Fan, H. Gu, "The

Impact of Artificial Intelligence and Blockchain on the Accounting Profession," IEEE Access, vol. 8, pp. 110461-110477, 2020.

[29] L. Zhong, Q. Wu, J. Xie, Z. Guan, B. Qin, "A secure large-scale instant payment system based on blockchain," Computers & Security, vol. 84, no. JUL., pp. 349-364, 2019.

[30] L. Zhong, Q. Wu, J. Xie, J. Li, B. Qin, "A secure versatile light payment system based on blockchain - ScienceDirect," Future Generation Computer Systems, vol. 93, pp. 327-337, 2019.