ISSN: 1813-4890

Optimizing data security and stability of blockchain technology in the global value exchange system

He Ji

Ukraine Odesa I. I. Mechnikov National University, Ukraine

501207117@qq.com

Abstract

The "blockchain" technology has gradually entered the lives of the public and become the focus of attention in society. Blockchain originated from Bitcoin and utilizes an encrypted chain blockchain structure to store data. Consensus algorithm is a core issue in blockchain technology. Using consensus algorithm to generate and validate data can effectively solve the problem of reliable transmission of trust and value on the Internet. However, in the value exchange system, blockchain has never truly been resolved and has achieved sufficient security. If its security and efficiency can be improved, it will greatly strengthen the fundamental tool effect in the global value exchange system

Keywords

Blockchain; Identification algorithm; Encryption technology.

1. Introduction

The blockchain technology value exchange system is a computer protocol aimed at disseminating, validating, or executing contracts in an information-based manner [1-3]. The most classic of these is that smart contracts allow for trusted transactions without a third party, which are traceable and irreversible.[4] The purpose of smart contracts is to provide better security methods than traditional contracts and reduce other transaction costs related to contracts. A smart contract is a set of commitments defined in numerical form, including protocols on which contract participants can execute these commitments [5].

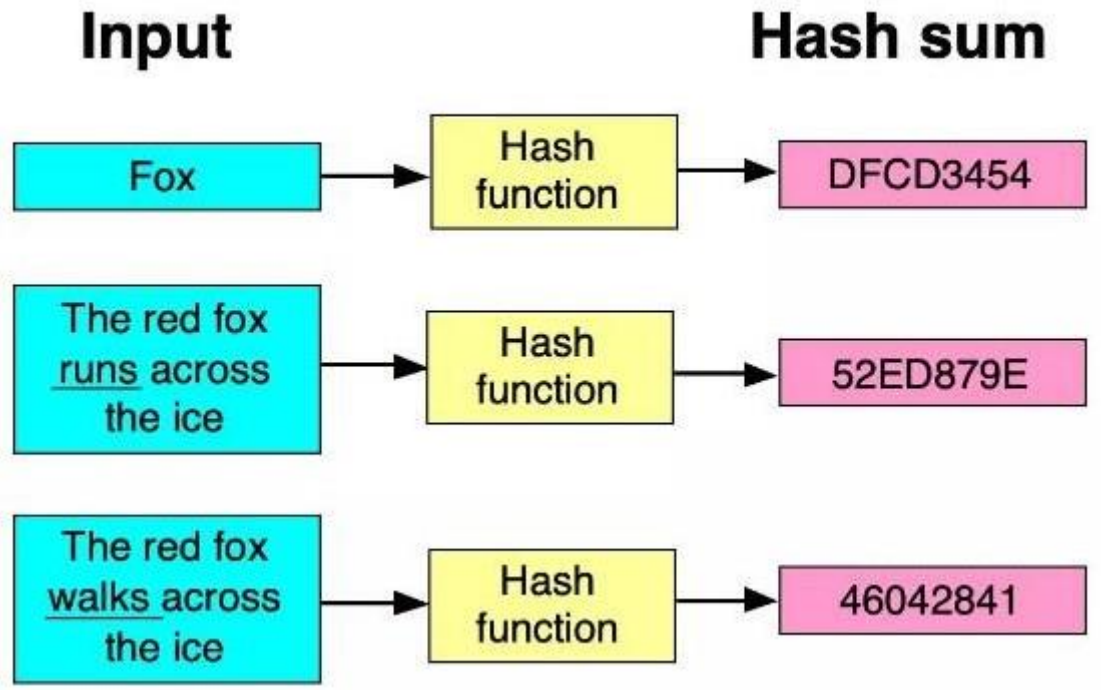
Due to the many advantages of using blockchain technology in value exchange and delivery systems. The advantages include decentralization, timestamp and irreversibility, openness, and convenience in the entertainment consumption system, while customers' consumption and entertainment come with a point effect. Blockchain technology is applied in value exchange systems, such as service exchange, commercial value exchange, and currency attribute value exchange [6]. From a commercial perspective, such systems come with inherent traffic and propagation attributes, but from a technical implementation perspective, there are still many hidden dangers and shortcomings [7]. Currently, there is no global trading currency in the game system.

2. Previous technical references and current major issues

2.1. Hash algorithm

The hash functions used in the Bitcoin system are used to perform workload proof calculations and generate addresses. In short, the hash algorithm maps any length string to a shorter fixed length string [8]. Due to the certainty and efficiency of this operation, decentralized computing can be achieved. Due to the sensitivity to input and the difficulty in finding the inverse function of the mapping (such as antigen attacks), it greatly contributes to the security of blockchain systems.

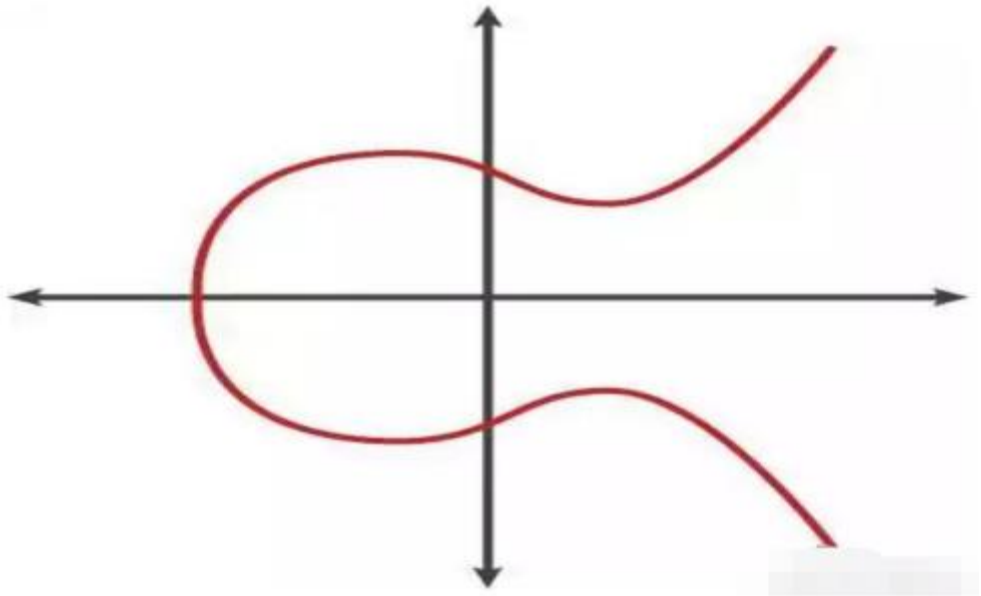
ISSN: 1813-4890



2.2. Elliptic curve algorithm

Elliptic curves are a set of algorithms for encrypting data, decrypting data, and exchanging keys, which can also be used for data signature and verification [9].

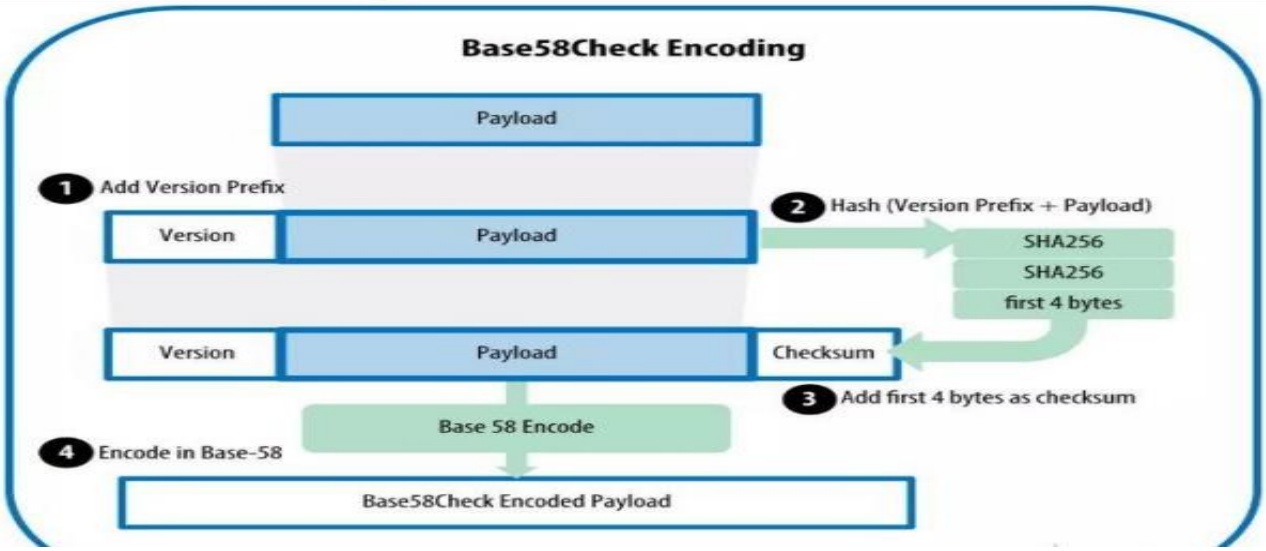
Signing can ensure that the user's account is not replaced by others, and on the other hand, it ensures that the user cannot deny the transaction they have signed [10]. Sign the transaction information with a private key, and the miner verifies the signature with the user's public key. If the verification is successful, the transaction information is recorded and the transaction is completed.



ISSN: 1813-4890

2.3. Base58 encoding

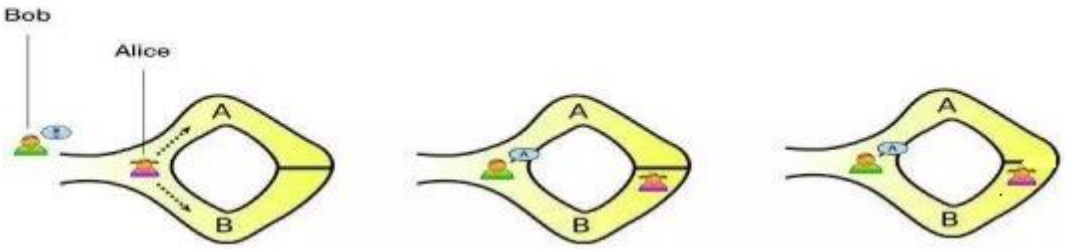
Base58 is the encoding method used by Bitcoin, mainly used to generate wallet addresses for Bitcoin. This encoding format not only achieves data compression, maintains readability, but also has error diagnosis function [11].



2.4. Zero knowledge proof

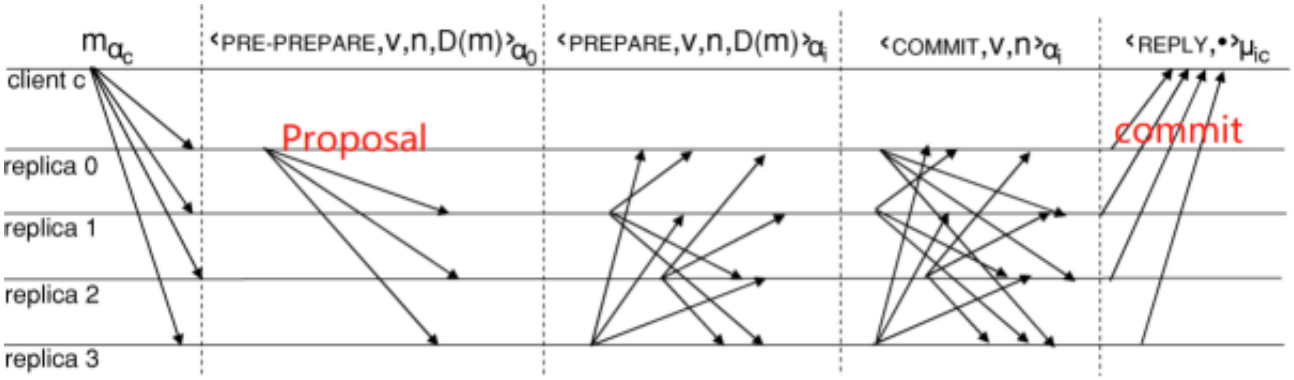
Zero knowledge proof is a technology jointly proposed by computer scientists Goldwasser and Micali in the early 1980s [12]. It mainly refers to the ability of the verifier to make the verifier believe that a certain statement is correct without providing any useful information to the verifie r[13].

Zero knowledge proof requires three elements to be established, namely completeness, reliability, and zero knowledge [14]. For example, suppose there is a circular corridor where the exit and entrance are adjacent but not interconnected (within a visual distance), and there is a locked door in the middle of this circular corridor that only those with keys can pass through; At this point, A needs to prove to B that he has the key to open this door, using zero knowledge proof to solve the problem. B watches A enter the entrance and wait at the exit [15]. If A enters through the corridor from the entrance and exits, it can prove that he has the key to open the middle door. In this process, he does not need to provide specific information about the key to B. So zero knowledge proof is actually a probability proof rather than a deterministic proof [16].



ISSN: 1813-4890

2.5. The PBFT (Practical Byzantine Fault Tolerance) algorithm is a distributed system consensus algorithm that can tolerate Byzantine errors.



2.6. Major issues

Blockchain technology is applied in value exchange systems, such as service exchange, commercial value exchange, and currency attribute value exchange[17]. The problem with the exchange of monetary attribute values is that the computational complexity is enormous, and the security of exchange of monetary attribute values has always been a problem For example, in 2014, the MT.GOX exchange in Japan was robbed of a total of 750000 Bitcoins, leading to the closure of the exchange. Although the hierarchical and layered design of blockchain computing and communication systems is perfect, the technology of segmented design is still incomplete. This can lead to a lack of response time and stability of computing nodes during the execution of concurrent tasks with huge computational workload[18]. The biggest advantage in blockchain technology 1.0 and 2.0 has become a systemic weakness in the later stages of development.

3. Recommendations for countermeasures

Optimize the Storage security and algorithm redundancy in the blockchain value exchange system, and improve the operating efficiency and security of system nodes facing concurrent big data[19].

The main tasks that need to be addressed to achieve the objectives of this study:

Strengthen the security of the value exchange system from the key or encryption algorithm in the underlying design, strengthen the security of the blockchain value exchange system from the design of information storage methods, and adopt optimization algorithms or replace old computing models with new mathematical models from the perspective of saving computing power at blockchain nodes[20]. Fundamentally solve the security issues of storage and value exchange from the perspective of algorithms or methods. Secondary tasks include the expectation of achieving pure value independence within the trading system, such as the exchange of value reflected in human social services.

There are optimizable methods or algorithms that can improve the security and speed of blockchain in value exchange systems in response to the shortcomings of existing 9 categories of methods or algorithms[21].The algorithms and methods currently awaiting research include:

The original password key was asymmetric encryption, but once the encryption or decryption key is obtained, these keys will all be public keys. We can divide the key into a public key and a secret key, [22]which can increase the security of the key thousands of times at a very small algorithmic cost.

Distributed information storage has its own advantages and supports the definition of decentralization. At the same time, it also brings more costs to centralized verification of

ISSN: 1813-4890

information, including time, computing power, loss of existence, and whether it is possible to create a specialized centralized service under transaction premise to reduce or eliminate such errors[23].

Previously, early value trading systems, such as Bitcoin, relied on computing power to create new value currencies in old systems, which was essentially a waste of money. Establishing a process of directly creating equivalents between the real and digital worlds would eliminate the waste of computing power and the fallacy of generating digital system wealth out of thin air[24], The meaning of this method, which I temporarily named "Real Digital Fruits", is that only the value in reality can give birth to the general equivalent of blockchain systems.

The world is originally a family, and improving the value exchange system of blockchain while establishing a universal currency for global gaming or entertainment systems is also a pioneering move.

If both parties breach the contract during the transaction, the platform will automatically call the smart contract to punish the defaulting party. The punishment will be in accordance with the

The smart contract has been written in advance, and once a breach occurs, a penalty for breach will be immediately executed, and the breach information will be broadcasted to the number of transactions involved

Synchronize updates based on all nodes on the chain, which will affect the user's comprehensive reputation value and serve as a consensus node selection service for future filtering

Based on this, to improve the success rate and credibility of transactions.

Algorithm Description

Due to the parallel multi chain blockchain model dividing the entire network nodes into multiple sub chains, the ability of each sub chain to resist malicious node attacks decreases. When the computing power of malicious nodes in the sub chain exceeds 51%, it can cause malicious nodes to collude in attacks. Therefore, this article proposes a network sharding algorithm (AANS) to resist collusion attacks. The AANS algorithm is described as shown in the algorithm.

Algorithm AANS algorithm

Input: Chain granularity m, number of blockchain

nodes n, node set V={v1,..., vi,..., vn},

computing power set P={p (v1),..., p (vi),..., p (vn)},

node trust integral set T={t (v1),..., t (vi),..., t (vn)}, trust threshold Tthreshold.

Output: Chain={VChain 1,..., VChain i..., VChainm} and calculate

Nr, Pr, Mr., Dr.VMal=, Chain=b)

For (i=0; i<n; i++)

If t (vi) ≥ Threshold then

VMal=VMal Å vi

End if

End for

C) for (i=0; i<num (VMal) -1; I++)

If p (vj) > p (vj+1) then

Swap the positions of vj and vj+1 in VMal

End if

End for

ISSN: 1813-4890

End for
d) For (i=0; i<num (VMal); I++)
K=i% m
VChaink=VChaink Å VMal (i)
End for
E) Random (VMal)
f) For (i=0; i<num (VMal); I++)
K=i% m
VChaink=VChaink Å VMal (i)
End for
g) Output Chain={VChain 1,..., VChain i,..., VChainm}
h) Calculate Nr, Pr, Mr, Dr according to the definition

The AANS algorithm comprehensively considers the behavioral and computational characteristics of nodes, and divides malicious nodes and honest nodes by polling all nodes in the blockchain network. At the same time[25], malicious nodes are evenly distributed among each sub chain based on their computing power values, ensuring a balanced

4. Conclusion

By analyzing the highest proportion of collusion computing power in sub chains with different granularity and malicious node ratios, it can be concluded that overall, the AANS algorithm has a relatively low proportion of collusion computing power and a lower risk of collusion attacks. However, the proportion of malicious node collusion computing power only brings the risk of collusion attacks. In order to further analyze the security of AANS algorithm, it is necessary to compare the proportion of sub chain collusion attacks under different granularity of chain partitioning. Set the malicious node ratio to 40%, and set the chain granularity to 3, 5, 7, and 10.

From Figure 8, it can be seen that under different chain granularity, the proportion of sub chain collusion attacks in Zilliqa and Omniledger is greater than 0, and both sub chains are attacked by malicious nodes in collusion. Among them, the Zilliqa algorithm accounts for 40% of malicious nodes, and when the chain granularity is 3, the proportion of sub chain collusion attacks reaches 67%. At this time, the proportion of sub chain collusion attacks by malicious nodes is the highest. However, the AANS algorithm only experienced collusion attacks when the granularity of the chain was 10, and there was no collusion attack problem in other cases.

In summary, through the above experimental analysis, it can be concluded that the AANS algorithm can evenly allocate malicious nodes and their computing power to each sub chain, reducing the aggregation of malicious nodes in the sub chain, avoiding the fluctuation of the proportion of collusive computing power, and effectively reducing the risk caused by collusive attacks in the sub chain

In order to address the scalability issues of blockchain, this article constructs a parallel multi chain performance optimization model from the perspective of modifying the underlying network architecture. This model improves the throughput of blockchain business processing and enhances the scalability of the system. On this basis, a network sharding algorithm (AANS) against collusion attacks is proposed to address the sub chain security issues in parallel multi chain blockchain models. This algorithm polls all malicious nodes in the blockchain network, evenly allocating malicious nodes and their computing power to each sub chain, preventing malicious nodes from occupying a large

number of sub chains, resulting in 51% attacks caused by malicious node computing power aggregation. The experimental results show that under different granularity of fragmentation, the sub chain collusion computational power and sub chain collusion attack proportion of AANS algorithm are lower than existing network fragmentation algorithms, which to some extent improves the security of parallel multi chain models. When designing the network sharding algorithm in this article, the trust threshold was used to determine whether a node is a malicious node. The evaluation criteria for node behavior characteristics were not specifically studied. Therefore, how to design a reasonable node behavior feature determination scheme to make the identification of malicious nodes more accurate is the direction of future research

5. Acknowledgements

I would like to thank my family and friends for their selfless support, encouragement, and research support. During this period, they provided me with unwavering support and understanding, encouraging me to continue pursuing knowledge and breakthroughs.Without their support and understanding, I would not be able to complete this paper.

Thank you to the professors of Odessa National University in Ukraine, Professor Eugene V. Malakhov and Professor Oleksandr Antonenko。

References

[1]YAGA D, MELL P, ROBY N, et al. Blockchain technology overview[R].National Institute of Standards and Technology, 2018.

[2] ZHANG L, LUO Y L, TAO F, et al. Cloud manufacturing: a new manufacturing paradigm[J]. Enterprise Information Systems, 2014, 8(2): 167-187.

[3] Intelligent Research View. Development status of China's cloud manufacturing industry in 2021 and comparative analysis of cloud manufacturing enterprises (Nancal Technology Co.,Ltd VS Hi-tech Control System Co., Ltd)[EB]. 2021.

[4] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.

[5] CAI X Q, DENG Y, ZHANG L, et al. Blockchain principle and core technology[J]. Chinese Journal of Computers, 2021, 44(1): 84-131.

[6] LI B H, ZHANG L, WANG S L, et al. Cloud manufacturing: a new service-oriented networked manufacturing model[J]. Computer Integrated Manufacturing Systems, 2010, 16(1): 1-7, 16.

[7] CAI T, LIN H, CHEN W H, et al. Efficient blockchain-empowered data sharing incentive scheme for Internet of Things[J]. Journal of Software, 2021, 32(4): 953-972.

[8] DAI H N, ZHENG Z B, ZHANG Y. Blockchain for internet of things: a survey[J]. IEEE Internet of Things Journal, 2019, 6(5): 8076-8094.

[9] TAN L, SHI N, YU K P, et al. A blockchain-empowered access control framework for smart devices in green internet of things[J]. ACM Transactions on Internet Technology, 2021, 21(3): 1-20.

[10] XIE M H, LI H Y, ZHAO Y J. Blockchain financial investment based on deep learning network algorithm[J]. Journal of Computational and Applied Mathematics, 2020, 372: 112723.

[11] SONG Y N, ZHANG F R, LIU C C. The risk of block chain financial market based on particle swarm optimization[J]. Journal of Computational and Applied Mathematics, 2020, 370: 112667.

[12]SHEN M, SANG A Q, ZHU L H, et al. Abnormal transaction behavior recognition based on motivation analysis in blockchain digital currency[J].Chinese Journal of Computers, 2021, 44(1): 193-208.

[13]YANG X D, XI W T, WANG J Q, et al. Electronic evidence sharing scheme of internet of vehicles based on signcryption and blockchain[J]. Journal on Communications, 2021, 42(12): 236-246.

ISSN: 1813-4890

[14] ZHANG J Y, WANG Z Q, XU Z L, et al. A regulatable digital currency model based on blockchain[J]. Journal of Computer Research and Development, 2018, 55(10): 2219-2232.

[15] ZHANG Q, LIAO B Y, YANG S L. Application of blockchain in the field of intelligent manufacturing: theoretical basis, realistic plights, and development suggestions[J]. Frontiers of Engineering Management,2020, 7(4): 578-591.

[16] VATANKHAH B R. A blockchain technology based trust system for cloud manufacturing[J]. Journal of Intelligent Manufacturing, 2022, 33(5): 1451-1465.

[17]JING N, LIU Q, SUGUMARAN V. A blockchain-based code copyright management system[J]. Information Processing & Management, 2021, 58(3): 102518.

[18] KARAFILOSKI E, MISHEV A. Blockchain solutions for big data challenges: a literature review[C]//Proceedings of IEEE EUROCON 2017-17th International Conference on Smart Technologies. Piscataway:IEEE Press, 2017: 763-768.

[19] LIU A D, DU X H, WANG N, et al. Blockchain-based access control mechanism for big data[J]. Journal of Software, 2019, 30(9): 2636-2654.

[20] KAMATH R. Food traceability on blockchain: walmart's pork and mango pilots with IBM[J]. The Journal of the British Blockchain Association,2018, 1(1): 1-12.

[21] WEI X, WANG X Y, YU Z, et al. Cross domain authentication for IoT based on consortium blockchain[J]. Journal of Software, 2021, 32(8): 2613-2628.

[22] CHEN Y R, CHEN H, HAN M, et al. Security consensus algorithm of medical data based on credit rating[J]. Journal of Electronics & Information Technology, 2022, 44(1): 279-287.

[23] LIN P, SONG Q Y, YU F R, et al. Task offloading for wireless VR-enabled medical treatment with blockchain security using collective reinforcement learning[J]. IEEE Internet of Things Journal, 2021, 8(21): 15749-15761.

[24] ZHANG C, LI Q, CHEN Z H, et al. Medical chain: alliance medical blockchain system[J]. Acta Automatica Sinica, 2019, 45(8): 1495-1510.

[25] LIU X L, BARENJI A V, LI Z, et al. Blockchain-based smart tracking and tracing platform for drug supply chain[J]. Computers & Industrial Engineering, 2021, 161: 107669.