DESIGN OF BLOCKCHAIN LEDGER COMPRESSION ALGORITHM

Zhijun Wu[1], Yiming Yang[1] and Xin Lu[2]

[1]College of Electronic Information and Automation, Civil Aviation University of China, Tianjin, China
[2]College of Economics and Management, Civil Aviation University of China, Tianjin, China

ABSTRACT

Blockchain has received widespread attention due to its decentralization, openness, autonomy, information tamper proof, and anonymity, and is currently on the rise. Some fatal weaknesses have been widely criticized in the process of evolution and development of blockchain technology. For example, the blockchain network has a large amount of data, large communication overhead, large storage overhead, and poor timeliness. The causes of these defects are complex, and the increase for data is the most important of many. In order to solve above problems, we research on the self-designed alliance chain that supports deletable ledger function, which can implement the function of searching and deleting ledger transactions. After the deletion request and execution are verified and agreed by the consensus nodes, the blockchain ledger is compressible or deletable. At the same time, the integrity of the forward and backward verification of the corresponding high-level blocks can be guaranteed without affecting the storage and usage of other blocks.

KEYWORDS

Blockchain, Deletable Ledger, Simulation Alliance Chain, Forward and Backward Verification

1. INTRODUCTION

Blockchain is a new type of decentralized infrastructure and distributed computing paradigm that gradually rises with the increasing popularity of digital cryptocurrencies. It is the underlying core technology of folk digital currencies such as Bitcoin, which integrates key technologies such as P2P networks, consensus mechanisms, and passwords. Blockchain technology has the characteristics of decentralization, immutability, anonymity, traceability, openness and transparency. The application prospects have attracted widespread attention from government departments, financial institutions, technology companies, and academia [1-3]. Taking the People's Bank of China as an example, it established a legal digital currency research group in 2014 to demonstrate the feasibility of legal digital currency issuance, published a number of related academic papers, and launched a prototype system of an electronic bill trading platform [4]. At the same time, many countries in the world currently have many blockchain experimental projects in many fields. Many blockchain alliances have been established internationally, such as the R3 alliance, Hyper Ledger, etc., with the aim of promoting the theoretical and applied research of blockchain technology [5]. In China, blockchain technology has risen to the level of national science and technology strategy [6].

Natarajan Meghanathan et al. (Eds) : CoSIT, AIAPP, SIGL, CRIS, DMA, NLPML, CYBI - 2020
pp. 71-80, 2020. © CS & IT-CSCP 2020 DOI: 10.5121/csit.2020.100107

Cryptography is one of the key technologies of the blockchain. It not only concerns the security and efficiency of the blockchain, but also the basic means to achieve the specific application of the blockchain. With the development of blockchain technology, some cryptographic technologies have been developing, further promoting the research of cryptographic theory and its applications [7]. More and more cryptographers have begun to pay attention to and study blockchain-related cryptography [8-9]. At present, the specific research includes the following two aspects: First, according to specific application requirements such as blockchain technology security analysis, consensus mechanisms, and privacy protection, cryptographers have made cryptographic algorithms and protocols (such as special digital signatures, zero-knowledge proofs, homomorphic encryption and secure multiparty computing) to conduct research [10-11]; Second, cryptographers use the decentralization, openness, transparency, and non-tampering of blockchain technology to build secure multiparty computing protocols and publicly verifiable random number seed, etc. [12].

It is well known that blockchain technology has a wide range of application prospects and is even considered a revolutionary technology, but its development is always accompanied by a complex and difficult problem [13]. While obtaining anti-counterfeiting security of the ledger, the amount of ledger data in all the various nodes of the blockchain network has only continued to increase, which has a significant efficiency impact on the application of system resources, network bandwidth and chain availability. In addition, the block where some invalid, illegal or redundant data is located will not only occupy a large amount of blockchain storage resources, but also bring potential troubles in terms of unpredictable laws and ethics. Based on this situation, this paper designed a cryptographic algorithm in the alliance chain that supports deletable ledger transactions, which can retrieve and delete confidential ledger transactions that meet the above hidden danger, but does not affect the corresponding high-level blockchain ledger. The integrity verification of the forward and backward block, the identity and authorization of the performer of the deletion operation can be verified by the consensus node of the alliance chain, and the algorithm speed test does not exceed the millisecond level, which has strong practical value.

2. KEY TECHNOLOGY

This paper is mainly aimed at the resource consumption caused by the unlimited growth of the blockchain ledger and the impact on the efficiency of the blockchain. The research design of the removable and compressible ledger is introduced below.

2.1. Design of Alliance Chain Experimental Platform

This paper bases on the self-designed alliance chain experimental platform. The platform has the main functional modules, which includes peer, wallet, multi-signature verification, data type, simulated network generation. The peer module mainly completes the four functions, wallet generation, routing, consensus and storage blocks. For example, specifically, the wallet generation function is used to generate the wallet address. The routing function realizes the most direct data transmission between all nodes in the entire network, verifies the validity of transactions and blocks, receives and sends valid transactions and legal blocks to other nodes in the network. The storage function is used to realize a complete, brand-new backup of blockchain data. Consensus function guarantees the consistency of blockchain data through consensus algorithms. The wallet module mainly implements some functions, such as creating transactions and querying balances. The multi-signature verification module is mainly used to delete or compress the identity of the operator of the block in the alliance chain and the consensus node of the alliance chain can verify the authorization. The data type module mainly specifies the data structure of each object in the blockchain. For example, in the simulation chain, a list is used to store the blockchain. Each element in the list represents a block, and the data structure of the block has different definitions depending on the type of block. The role of the simulated network generation module is to generate a virtual P2P network, which is only a topological mapping of the real network.

The organizational structure of the alliance chain experimental platform is shown in Table 1:

Table 1. Organization structure of the experimental platform

Module	**Function**
network.py	Define the simulated network objects
peer.py	Define the peer objects
wallet.py	Wallet Objects
ecc.py	Related objects of Elliptic Curve Cryptography
consensus.py	Consensus Algorithm
datatype.py	Basic data types
vm.py	Stack machine
params.py	Define the basic parameters
logger.py	Recorder
merkletree.py	Defined the object of Merkel tree
base58.py	base58 module
ptsh.py	Multi-signature module

2.2. Encryption and Signature Algorithms of the Alliance Chain

In the established alliance chain, this paper uses the ECC elliptic curve encryption algorithm to generate the wallet address of each node of the blockchain network and perform the signature and verification signature functions.

ECC is different from traditional encryption methods based on the difficulty of large prime factorization. The key pair is generated from the properties of the elliptic curve equation. ECC164-bit keys generate a security level, which is equivalent to the security strength provided by RSA's 1024-bit keys. Moreover, the calculation amount is small, the processing speed is faster, the storage space and transmission bandwidth occupy less, and the virtual currency Bitcoin also chooses ECC as the encryption algorithm.

This paper uses the secp256k1 curve with the following parameters:

$$\begin{aligned}&p = 0\text{xFFFFFFFFFFFFFFFFFFFFFFFFFFFFF}\\&\text{FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC2F}\\&\quad = 2^{256} - 2^{32} - 2^{9} - 2^{8} - 2^{7} - 2^{6} - 2^{4} - 1\end{aligned}$$

2.3. Design of Functions

This paper researched the problem of blockchain scale expansion, and mainly achieved the three functions of deletion, compression and retrieval.

The overall design flowchart of this paper is shown in Figure 1.

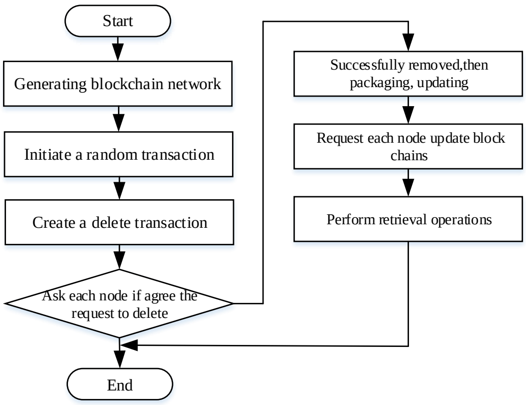

Start
Generating blockchain network
Initiate a random transaction
Create a delete transaction
Ask each node if agree the request to delete
Successfully removed,then packaging, updating
Request each node update block chains
Perform retrieval operations
End

Figure 1. Design flowchart

2.3.1. Delete Function

The delete function designed in this paper is to delete one or more consecutive blocks in the blockchain and generate a new deleted block at the same time to replace the one or more deleted sub-chain. The delete operation is shown as Figure 2.

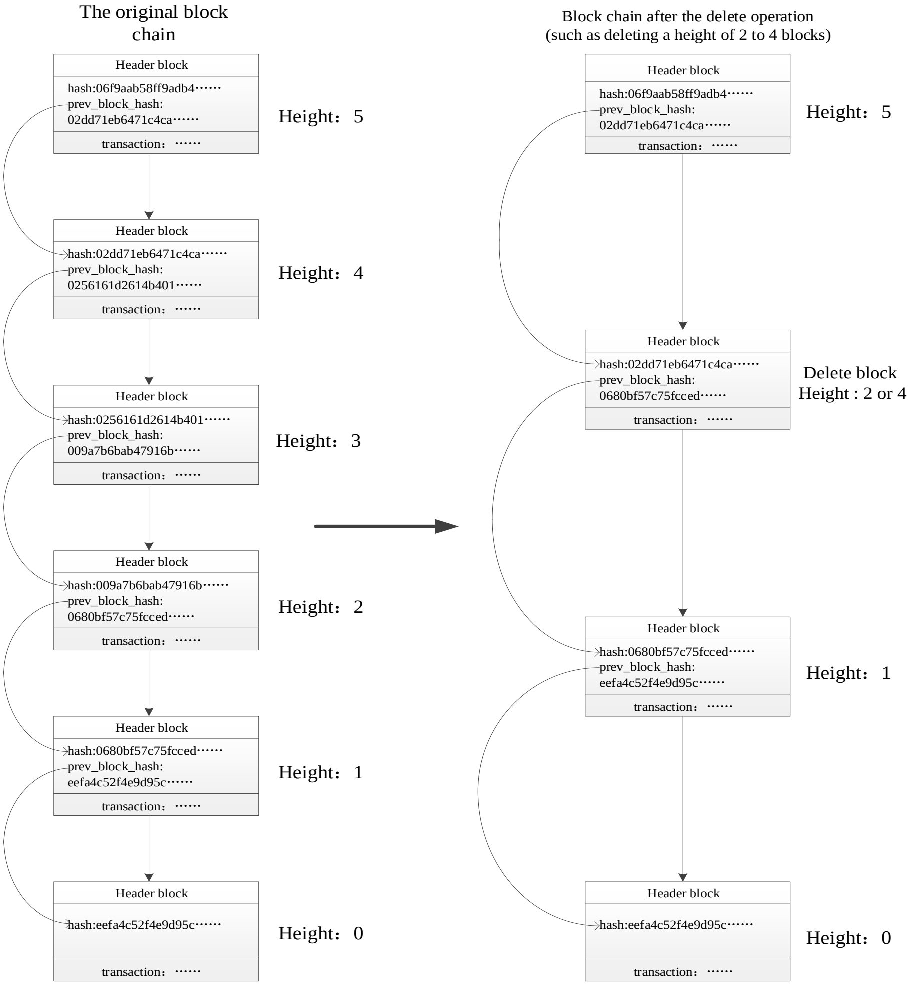


Figure 2. Schematic diagram of delete operation

To ensure the deletion that is the forward block hash value of the block is the same as the forward block hash value of the deleted block or the starting block of the blocks. The block height of the deleted block is the same as the block height of the start block or the end block of the block sub-chain. The hash value of this block of the deleted block is the same as the block hash value of the deleted block or the termination block of the block sub-chain. Not only can the ledger be deleted, but also the integrity verification of the forward and backward blockchain of the corresponding high-level blockchain ledger can be satisfied. In particlur, the forward and backward verification in this paper is achieved by defining the data structure of the deleted block. Hence, worrying about hash collisions is superfluous. Once the delete transaction is started, the design idea of this paper is to return two hash values in preparation for the use of the deleted block. One of the two returned hash values is the forward hash value of the deleted block segment, and the other is the hash value of the last block of the segment. As for the security and anti-attack of this operation, it is the current research focus.

2.3.2. Compress Function

The compress operation is similar to the delete operation. First, the continuous block sub-chain to be compressed is stored offline, and then the same operation as the delete block sub-chain is performed. After the execution of the delete operation is completed, the size of the block is compressed.

2.3.3. Retrieval Function

The realization of the retrieval operation needs to locate the target block which has the target transaction, and then obtain the position of the transaction that is required to be retrieved through the Merkel tree. At last, the transaction retrieval function can be completed. The retrieval operation is shown as Figure 3.

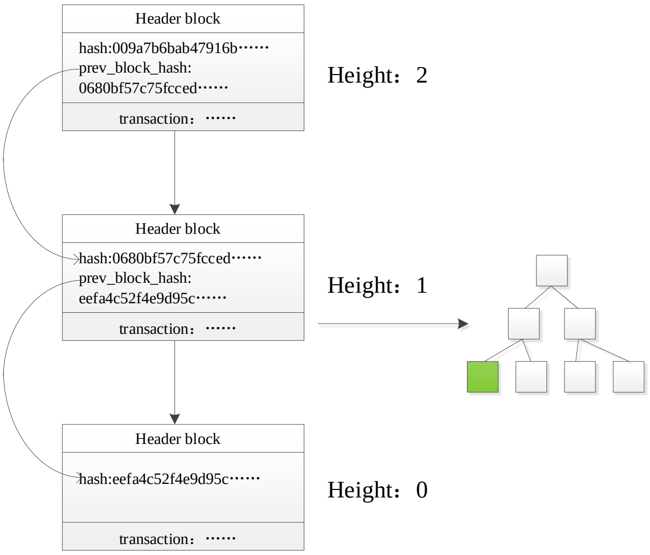


Figure 3. Retrieval operation diagram

3. EXPERIMENTS AND RESULTS ANALYSIS

This paper is mainly designed to realize deletion, compression and retrieval functions. The following is a functional and performance test based on the three functions in the alliance chain experimental platform. The operating environment of the Alliance Chain experimental platform is

Intel (R) Core (TM) i5-3210M CPU @ 2.50GHz dual-core laptop, and each module is implemented using Python language version 3.6.5.

3.1. Time Test of Block Generation

First test the time it takes in the alliance chain with 5 nodes to generate different numbers of blocks, as shown in Figure 4.

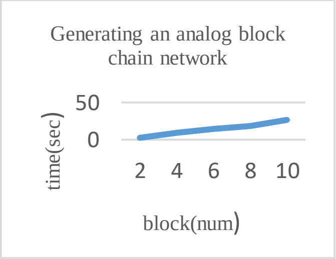


Figure 4. Generate blocks time

As can be seen from the Figure 4, when there are 5 nodes in the alliance chain, the average time taken to generate a new block is about 2.34s, and the transaction time is relatively shorter, which can meet the actual needs of blockchain transactions.

3.2. Time Test of Delete Block Operation

Test the time it takes to delete a different number of blocks, as shown in Figure 5.

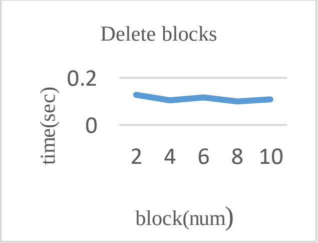
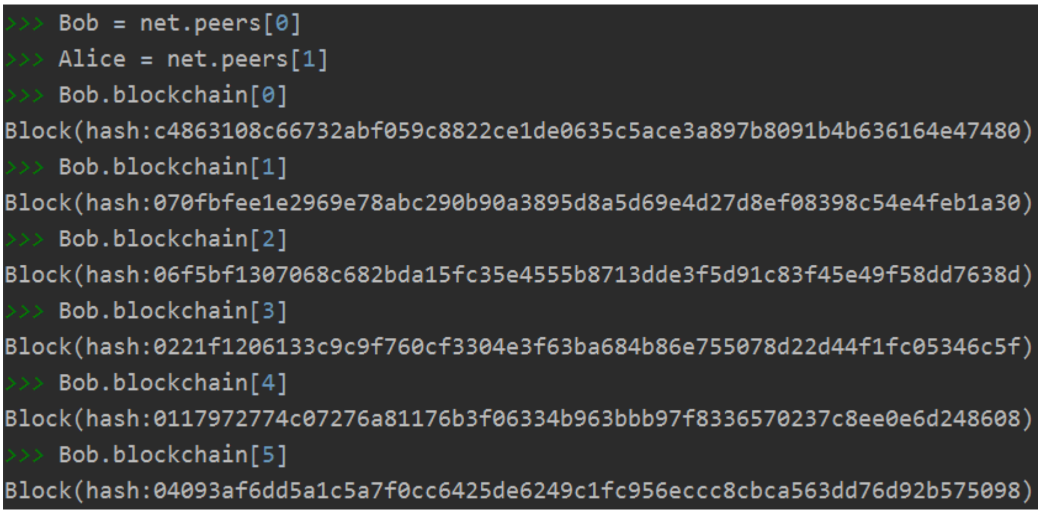


Figure 5. Delete blocks time

It can be concluded that the number of deleted blocks is not directly related to the time it takes. No matter how many blocks are deleted, the execution time of the delete operation can always be maintained in the millisecond level, which can meet the time requirements of practical applications.

3.3. The Test of Forward and Backward Verification

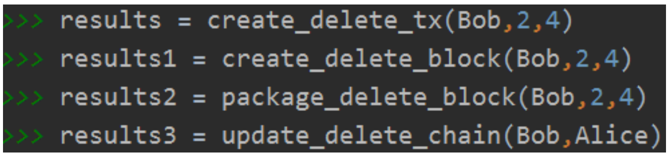
This test mainly tests the integrity of the forward-backward verification between blocks after the block deletion operation. Only the delete operation would meet the forward-backward, can it be explained that the delete operation is actually completed without affecting normal operation of other blocks. As shown in Figure 6, the current height of the blockchain is 5, and the blockchain remains intact.



```
>>> Bob = net.peers[0]
>>> Alice = net.peers[1]
>>> Bob.blockchain[0]
Block(hash:c4863108c66732abf059c8822ce1de0635c5ace3a897b8091b4b636164e47480)
>>> Bob.blockchain[1]
Block(hash:070fbfee1e2969e78abc290b90a3895d8a5d69e4d27d8ef08398c54e4feb1a30)
>>> Bob.blockchain[2]
Block(hash:06f5bf1307068c682bda15fc35e4555b8713dde3f5d91c83f45e49f58dd7638d)
>>> Bob.blockchain[3]
Block(hash:0221f1206133c9c9f760cf3304e3f63ba684b86e755078d22d44f1fc05346c5f)
>>> Bob.blockchain[4]
Block(hash:0117972774c07276a81176b3f06334b963bbb97f8336570237c8ee0e6d248608)
>>> Bob.blockchain[5]
Block(hash:04093af6dd5a1c5a7f0cc6425de6249c1fc956eccc8cbca563dd76d92b575098)
```

Figure 6. Blockchain status before delete operation

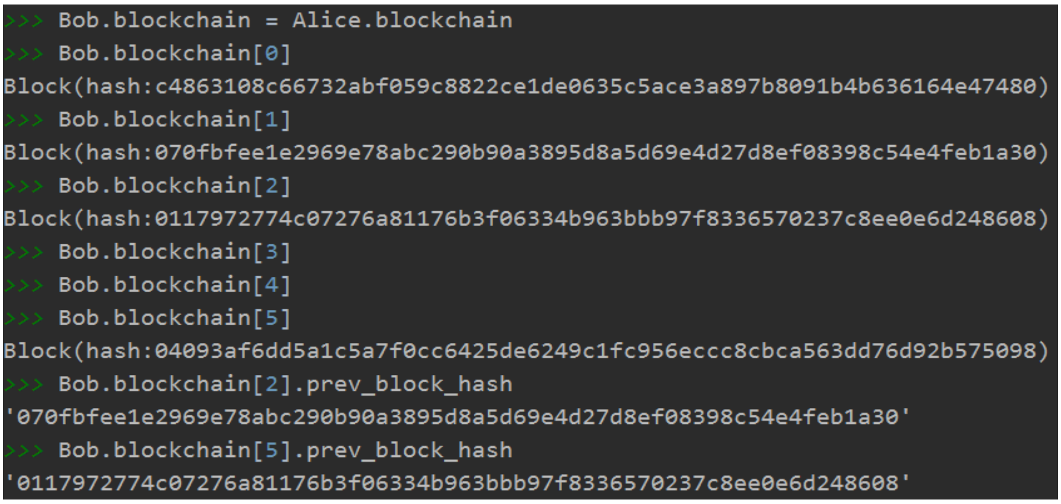
Next, the node in the blockchain network, Bob, initiates a request to delete three blocks with the block height of 2 to 4. After each node of the blockchain network passes the verification, Bob initiates a delete transaction locally and packages the delete block, and finally Bob asks Alice to update the new blockchain synchronously by herself. The operation command is shown in Figure 7.



```
>>> results = create_delete_tx(Bob,2,4)
>>> results1 = create_delete_block(Bob,2,4)
>>> results2 = package_delete_block(Bob,2,4)
>>> results3 = update_delete_chain(Bob,Alice)
```

Figure 7. Delete block operation

After the execution of the delete operation, check the state of the blockchain again to find that the blocks with block height 3 and 4 have disappeared, and the block with block height 2 is the new delete block that is packaged with delete transaction. The forward hash values of the blocks of 2 and 5 can be found as before, indicating that the entire delete operation does not affect the normal operation of the blockchain, as shown in Figure 8.

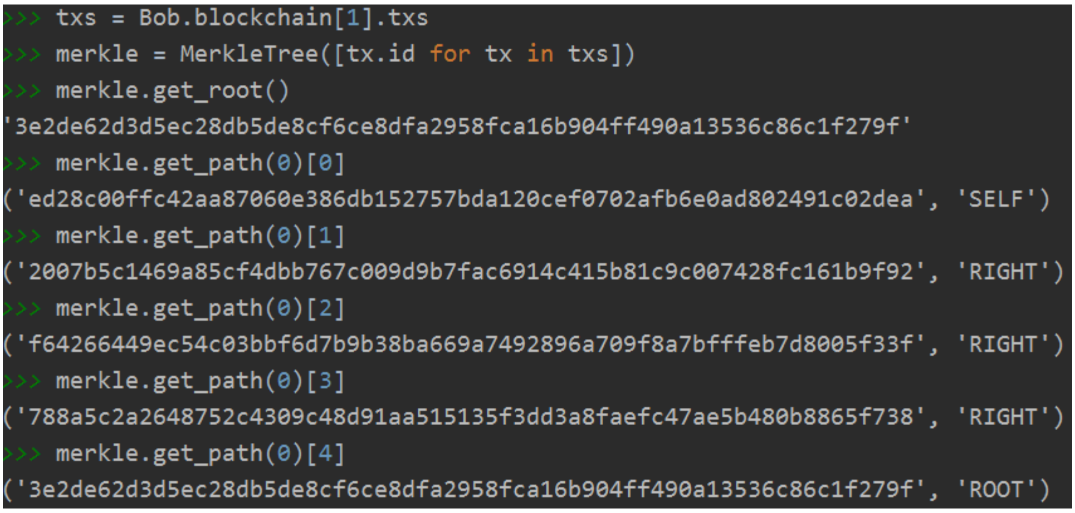


```
>>> Bob.blockchain = Alice.blockchain
>>> Bob.blockchain[0]
Block(hash:c4863108c66732abf059c8822ce1de0635c5ace3a897b8091b4b636164e47480)
>>> Bob.blockchain[1]
Block(hash:070fbfee1e2969e78abc290b90a3895d8a5d69e4d27d8ef08398c54e4feb1a30)
>>> Bob.blockchain[2]
Block(hash:0117972774c07276a81176b3f06334b963bbb97f8336570237c8ee0e6d248608)
>>> Bob.blockchain[3]
>>> Bob.blockchain[4]
>>> Bob.blockchain[5]
Block(hash:04093af6dd5a1c5a7f0cc6425de6249c1fc956eccc8cbca563dd76d92b575098)
>>> Bob.blockchain[2].prev_block_hash
'070fbfee1e2969e78abc290b90a3895d8a5d69e4d27d8ef08398c54e4feb1a30'
>>> Bob.blockchain[5].prev_block_hash
'0117972774c07276a81176b3f06334b963bbb97f8336570237c8ee0e6d248608'
```

Figure 8. Verifying the forward and backward Hash consistency of a block

3.4. The Test of Retrieval Function

Here, the test retrieves the first transaction in a block with the height 1, and the location of the target transaction can be easily found through the Merkel tree, as shown in Figure 9.



```
>>> txs = Bob.blockchain[1].txs
>>> merkle = MerkleTree([tx.id for tx in txs])
>>> merkle.get_root()
'3e2de62d3d5ec28db5de8cf6ce8dfa2958fca16b904ff490a13536c86c1f279f'
>>> merkle.get_path(0)[0]
('ed28c00ffc42aa87060e386db152757bda120cef0702afb6e0ad802491c02dea', 'SELF')
>>> merkle.get_path(0)[1]
('2007b5c1469a85cf4dbb767c009d9b7fac6914c415b81c9c007428fc161b9f92', 'RIGHT')
>>> merkle.get_path(0)[2]
('f64266449ec54c03bbf6d7b9b38ba669a7492896a709f8a7bfffeb7d8005f33f', 'RIGHT')
>>> merkle.get_path(0)[3]
('788a5c2a2648752c4309c48d91aa515135f3dd3a8faefc47ae5b480b8865f738', 'RIGHT')
>>> merkle.get_path(0)[4]
('3e2de62d3d5ec28db5de8cf6ce8dfa2958fca16b904ff490a13536c86c1f279f', 'ROOT')
```

Figure 9. Retrieving transaction operation

4. CONCLUSIONS

The research work in this paper is mainly aimed at the problems of invalidity in the blockchain, large resource consumption caused by the accumulation of illegal or redundant data, and the design of an ledger compression algorithm to solve the above problems. It was a cryptographic algorithm capable of deleting ledger transactions, designed by the self-designed alliance chain experimental platform. The algorithm can support retrieval and deletion of ledger transactions, and delete operations can only be performed after the consensus nodes have verified and agreed. The integrity of the forward and backward block verification of the high-level blockchain ledger does not affect the storage and usage of other blocks, and the algorithm rate is below the millisecond level. The experimental results show that the scheme designed in this paper can meet the actual requirements of social production, has good test performance, and has certain reference value in the actual application of the blockchain technology.

ACKNOWLEDGEMENTS

This work was supported in part by the joint funds of National Natural Science Foundation of China and Civil Aviation Administration of China (Grant No. U1933108), the Scientific Research Project of Tianjin Municipal Education Commission (No. 2019KJ117), the Fundamental Research Funds for the Central Universities of China (3122018D34007 and 3122018C003).

REFERENCES

[1] S. Nakamoto, (2008) "Bitcoin: A Peer-to-peer Electronic Cash System".

[2] I. Miers, C. Garman, M. Green and A. D. Rubin, "Zerocoin: Anonymous Distributed E-Cash from Bitcoin,"*2013 IEEE Symposium on Security and Privacy*, Berkeley, CA, 2013, pp. 397-411.

[3] E. B. Sasson et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin,"*2014 IEEE Symposium on Security and Privacy*, San Jose, CA, 2014, pp. 459-474.

[4] Y. Yuan, F. Wang, (2016) "Blockchain: The State of the Art and Future Trends", *ACTA AUTOMATICA SINICA*, Vol. 42, No. 4, pp.481-494.

[5] E. Androulaki, A. Barger, V. Bortnikov, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. in: Rui Oliveira, Pascal Felber, Y. Charlie Hu eds. Euro Sys'18 Proceedings of the Thirteenth Euro Sys Conference. Porto, Portugal, 2018. New York, NY, USA: ACM, 2018.

[6] China Blockchain Technology and Industry Development Forum, (2016) China Blockchain Technology and Application Development White Paper.

[7] A. Chauhan, O. P. Malviya, M. Verma and T. S. Mor, "Blockchain and Scalability," *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, Lisbon, 2018, pp. 122-128.

[8] A. Narayanan, J. Bonneau, E. Felten, et al. (2016) *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton University Press.

[9] M. Boniface et al., "Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds," *2010 Fifth International Conference on Internet and Web Applications and Services*, Barcelona, 2010, pp. 155-160.

[10] Y. Jiang et al., (2019) "A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management", *Sensors*, Vol. 19, No. 9, pp. 2042.

[11] H. Hong, B. Hu and Z. Sun, (2019) "Toward secure and accountable data transmission in Narrow Band Internet of Things based on blockchain", *International Journal of Distributed Sensor Networks*, Vol. 15, No. 4.

[12] H. Yi, (2019) "Securing e-voting based on blockchain in P2P network", *EURASIP Journal on Wireless Communications and Networking*, Vol. 2019, No. 1.

[13] F. Hawlitschek, B. Notheisen and T. Teubner, (2018) "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy", *Electronic Commerce Research and Applications*, Vol. 29, pp. 50-63.

AUTHORS

Zhijun Wu received the BS and MS degrees in Infor-mation Processing from Xidian University, China, and Ph.D. degree in Cryptography from Beijing University of Posts & Telecommunications, China. He is a profe-ssor in the College of Electronic Information and Aut-omation, Civil Aviation University of China. His rese-arch areas are denial-of-service attacks, security in big data and cloud computing.

Yiming Yang received the BS degree from Tianjin U-niversity of Commerce, China in 2017. She is working toward MS degree in Civil Aviation University of Ch-ina. Her research areas are blockchain and information security.

Xin Lu received the BS degree from China West Nor-mal University, China in 2016. He is working toward MS degree in Civil Aviation University of China. His research areas are blockchain and information security.