Framework of Energy Transaction Security Verification based on Blockchain

Shaomin Zhang, Cong Hou

School of Control and Computer Engineering, North China Electric Power University, Hebei Baoding 071003, China.

Abstract

Due to the limitation of blockchain performance, blockchain has not been used in large-scale business. In order to achieve safe and reliable energy trading in blockchain system, the communication efficiency, scalability and security indicators of blockchain are summarized. Based on the research summary of blockchain performance optimization, the energy trading framework is designed. Finally, simulation of energy trading scenarios, test the feasibility and security of the model, experiments show that the framework can identify the fake data of nodes, which is helpful to improve the security of energy trading.

Keywords

Energy Transaction; Blockchain; Security; Data Validity.

1. Introduction

Due to the limited performance of blockchain, there has been no large-scale commercial application. In the distributed system, due to the cap (consistency, availability, partition tolerance) theory, the three can only meet two of them at the most at the same time. Therefore, the performance optimization of blockchain has always been the focus of research. In the research of performance optimization, the communication efficiency, scalability and security mechanism of blockchain are the research hotspots.

1.1. Communication efficiency

In distributed systems, more and more attention is paid to the timeliness and reliability of data interaction experience. However, the efficiency of transaction processing is often restricted by the efficiency of data communication between the nodes of blockchain.

To solve the problem of data transmission in blockchain, a communication scheme based on node trust and weight is proposed in reference [1], which improves the communication efficiency between nodes. Reference [2] proposes to combine blockchain technology with Internet of things technology to improve the security of Internet of things data sharing, and give incentives to users who provide data. In this model, in order to improve the performance of blockchain, the consensus mechanism is improved and deployed to cloud / edge server, which improves the economic efficiency and communication performance.

1.2. Scalability

With the increasing number of transactions to be processed on the blockchain, the transaction processing capacity limits the application of payment scenarios. Blockchain expansion is the first problem to be solved, including the improvement of transaction throughput and the reduction of transaction confirmation delay.

Reference [3] points out that the scalability of blockchain limits the further development of blockchain technology, and points out the problems faced by the current solutions from the two improvement schemes of offline storage and online storage. Reference [4] analyzes the

ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0017

scalability problem from three aspects: consensus mechanism, block and transaction. Reference [5] improves the scalability of blockchain based on fragmentation technology, predicts the size of the optimal fragmentation, and enhances the scalability and throughput of blockchain.

1.3. Security

In recent years, blockchain projects have been attacked many times, and smart contract vulnerabilities have led to the theft of trading platforms. In 2016, hackers used smart contract vulnerabilities to attack the Dao, a crowdfunding project of decentralized autonomous organization (DAO), resulting in the transfer of more than 3 million Ethernet coins. These attacks have aroused public doubts about the security of blockchain.

Reference [6] proposed the security objectives of blockchain, namely data security, consensus security, privacy protection and smart contract security, analyzed the common security problems of blockchain system, the threat of quantum computing to cryptographic algorithm, the loss of user's secret key, imperfect formal verification and other problems, and pointed out the common attack paradigms against blockchain system, For example, dictionary attack against user secret key, distributed denial of service (DDoS) attack against peer-to-peer network, and nothing at make attack against consensus mechanism. Reference [7] attacks BTC network through eclipse attack, quantifies the resources involved in the attack combined with probability analysis and Monte Carlo simulation, and puts forward corresponding countermeasures.

2. Methodology

2.1. Design of model framework

According to the relevant technologies adopted by the energy blockchain, the model can be divided into five layers, namely: data layer, network layer, consensus layer, contract layer and application layer. This section will describe the improvement of each layer in detail.

Data layer: from Genesis block to the latest block, all energy trading information is stored through the data layer and connected through the chain structure. The data layer is the underlying data structure of the whole distributed energy data interchange model. In this model, the data layer includes distributed generation capacity data, transaction information data, user account information, hash value, timestamp, random number, etc. (as shown in Figure 1).

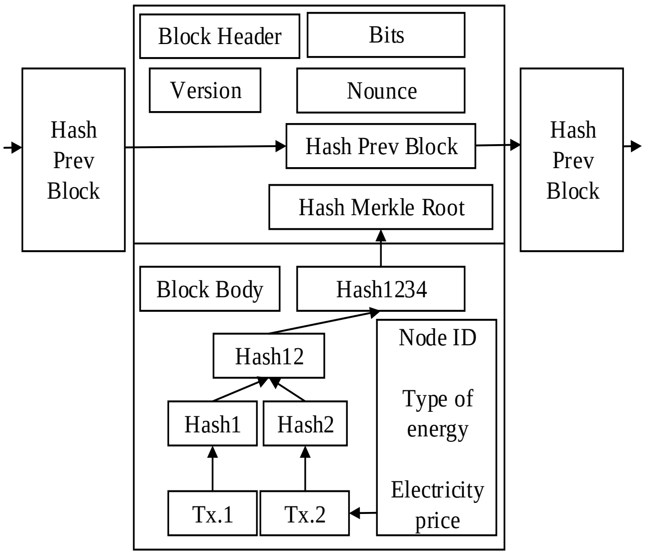


Figure 1. Data structure of energy blockchain

ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0017

Network layer: the model network consists of two aspects: the power network on the physical level and the blockchain network on the information level. Due to the characteristics of distributed generation, such as wide distribution, large base, easy to be affected by the environment, this model constructs the corresponding energy chain according to the different types of energy,in order to meet the requirements of system scalability and high transaction throughput, and realizes cross link transaction of heterogeneous energy data.

Consensus layer: consensus mechanism is the core of the whole model. Through the specified consistency protocol run by each node of the blockchain, the unified ledger can be achieved on the basis of certain fault tolerance. This consistency protocol is called consensus algorithm. In order to meet the requirements of transaction efficiency and security, this model is improved based on PoS and PBFT consensus mechanism. The data validity verification mechanism is introduced to improve the security of energy trading.

Contract layer: the smart contract allows transactions without endorsement from a trusted third party to achieve data traceability. Smart contracts with various functions can be designed according to the system requirements, such as user identity authentication smart contract, energy trading smart contract, power grid security check smart contract, etc. these smart contracts are deployed in the energy blockchain system, which can be automatically executed when the trigger conditions are met, without the intervention of intermediary agencies, reducing the impact of human factors on the system.

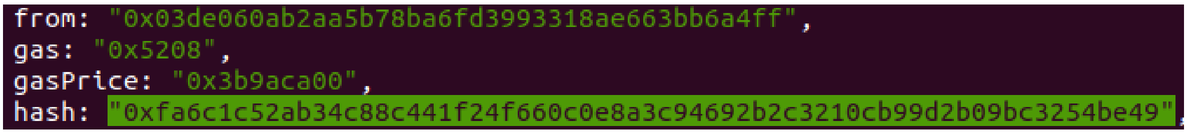
Application layer: energy blockchain system is closely connected with users through application layer, which is the window for energy blockchain system to provide various services. Through data visualization technology, a variety of decentralized applications (DAPP) can be installed on the user side, realizing the functions of complementary distributed energy and data interchange, which is convenient for users.

3. Results and discussion

3.1. Safety analysis

Finally, in order to verify the feasibility of the mechanism described in this paper, this section in the laboratory environment, based on the vscode development tool, download the solid development plug-in, install node.js, and build the private chain based on the truffle framework. Trading smart contract is released to the private chain as an energy Internet power trading platform to simulate the energy Internet scenario for simulation test.

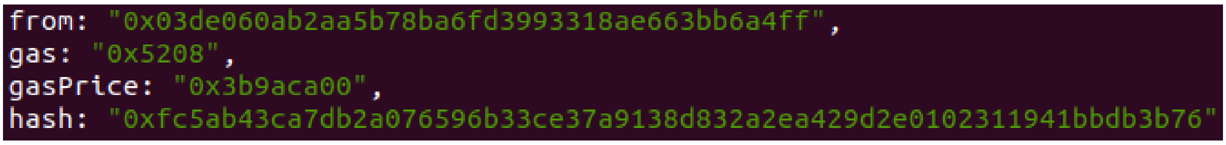
In the above experimental environment, the security is analyzed. Assuming that there are cheating nodes in the system, the fake energy transaction data is constructed in the block, and then the block containing the fake transaction is submitted to other nodes for verification. The submitted transaction data is shown in Figure 2.



```
from: "0x03de060ab2aa5b78ba6fd3993318ae663bb6a4ff",
gas: "0x5208",
gasPrice: "0x3b9aca00",
hash: "0xfa6c1c52ab34c88c441f24f660c0e8a3c94692b2c3210cb99d2b09bc3254be49",
```

Figure 2. Falsified transaction data

The honest node also maintains an account book containing global transaction data locally. When the honest node finds that the transaction data submitted by the cheating node is different from its own local data (the hash of the two transactions data can be compared through query), the honest node will actively send a message to other nodes to report the possible cheating behavior. The local energy trading data maintained by the honest node is shown in Figure 3.



```
from: "0x03de060ab2aa5b78ba6fd3993318ae663bb6a4ff",
gas: "0x5208",
gasPrice: "0x3b9aca00",
hash: "0xfc5ab43ca7db2a076596b33ce37a9138d832a2ea429d2e0102311941bbdb3b76"
```

Figure 3. Transaction data maintained by local nodes

After receiving the message sent by the honest node, other nodes judge the security status of transactions in the blockchain by comparing with the data received before. If the hash of the two energy trading data are not equal, the capital transaction on the blockchain will be stopped and further investigation will be conducted. Experiments show that the security verification framework can prevent malicious nodes from forging data and improve the security of energy trading.

4. Conclusion

As more and more distributed generation is integrated into the power grid, the problem of data interoperability in energy Internet becomes more and more prominent. In addition, with the increasing complexity of energy network structure, it also leads to many data security problems. In this paper, combined with the research of energy blockchain at home and abroad, according to the actual problems existing in the current energy Internet data interchange, an energy trading framework is designed to enhance security, the functions of each part are specified, finally,the security is analyzed to verify the feasibility of the model design scheme.

References

[1] J. Li, G.Q. Liang, T.S. Liu, X.J. Li (2017). P2P multicast algorithm considering node service priority. Application Research of Computers, vol. 34, no. 4, pp. 1176–1179.

[2] T. Cai, H. Lin, W.H. Chen, Z.B. Zheng, Y. Yu (2021). Efficient Blockchain-empowered Data Sharing Incentive Scheme for Internet of Things. Journal of Software, vol. 32, no. 4, pp. 953–972.

[3] Z.X. Sun. X. Zhang (2021) .Survey of Storage Scalability on Blockchain. Journal of Software,vol. 32, no. 1, pp. 1–20.

[4] Z.L. Mao, Y.N. Liu (2020). Research on Blockchain Performance Scalability and Security. Netinfo Security, vol. 20, no. 3, pp. 56–64.

[5] Y.L. Zeng (2020). Research on Block Structure Supporting High Throughput Blockchain [D]. University Of Electronic Science And Technology Of China.

[6] X. Han, Y. Yuan, F.Y. Wang (2019). Security Problems on Blockchain: The State of the Art and Future Trends. Acta Automatica Sinica, vol. 45, no. 1, pp. 206–225.

[7] Heilman E, Kendler A, Zohar A, Goldberg S. Eclipse attacks on bitcoin's peer-to-peer network. In: Proceedings of 24th USENIX Security Symposium. Washington, D.C, USA: USENIX, pp. 129-144,2015.