EasyChair Preprint

№ 6719

# Online Trading Platform for Power Company Suppliers Based on Blockchain Technology

Jijun Wang, Menghan Xu and Minsheng Xu



September 28, 2021

# Online trading platform for power company suppliers based on blockchain technology[1]

**Jijun Wang[2], Menghan Xu[1], Mingsheng Xu[3]**

[1]State Grid Jiangsu Electric Power Co., Ltd. Information & Techcommunication Branch , Nanjing Jiangsu, China

[2]Jiangsu Electric Power Information Technology Co., Ltd., Nanjing Jiangsu, China

[3]Jiangsu Electric Power Information Technology Co., Ltd., Nanjing Jiangsu, China

**Abstract:** In order to establish a reliable Electricity online trading system, this study constructs a decentralized traceability system based on the idea of blockchain. By storing and verifying the data of electricity supply chain on Kadelima distributed peer-to-peer network and Ethereum, a user data query service system is proposed.

**Keywords:** Smart contract, Blockchain, Trading System

## 0 Introduction

Blockchain computing makes the information Internet begin to transform into value Internet, which is usually used in the financial field and currency transactions, and is the mainstream direction of modern digital currency development. The core technology of blockchain has the advantage of decentralized design[1]. Based on cryptography, using encryption algorithm, time encryption and so on, and then through the distributed multi-node "consensus" mechanism, the whole transaction process can be recorded "completely" and "unalterable".

Blockchain includes data layer, network layer, consensus layer, incentive layer, contract layer and application layer. Nowadays, most blockchain technologies take advantage of its security. [2] [3] Blockchain adopts consensus mechanism to ensure that the global ledger maintained by all legal nodes is the same, based on POW mechanism， [4] the consensus mechanism is that by setting mathematical puzzles, the participating nodes can solve the puzzles, and the nodes that pay the most computing power can be regarded as several nodes, and then new blocks can be generated. In contrast, in order to reduce the consumption of computing power, POS mechanism [5] select the mechanism node by the number of days of currency holding. Computing power is a big problem in blockchain. [6] In order to solve the problem of slow query speed in blockchain, a DB architecture is proposed, which improves the speed by adding an analysis layer to the consensus layer. document[7]By expanding the blockchain architecture of loamit, the index of all blocks is constructed by adding time range

[1] Fund Project Name: Research and Application of Data Security Protection Technology Based on Data Center
Fund Project No: 5210ED2100L

and space threshold to the bottom of each blockchain, and some literatures put forward the blockchain based on undirected graph. [9] An extensible Block-DAG protocol called PHANTOM is proposed, which greatly improves the transaction speed. On the other hand, most Block-DAG protocols use Gossip algorithm. [10] To ensure the final consistency between different transactions. There are also research tasks, in order to ensure the security of blockchain technology, to model smart contracts and study their security. Fan Jili et al. [11] In the summary of smart contract technology, it is pointed out that the on-line projects that once had smart contracts were forced to suspend due to the high gas consumption at runtime. At the same time, they also believe that formal verification as the main representative of the code review method can more effectively find the loopholes in the contract code. Cao Yi et al. [12] It is considered that there are timestamp dependence, intrusion vulnerability and call stack depth in smart contracts. At the same time, the difference between security and privacy is discussed: security mainly refers to possible attacks; Privacy refers to the disclosure of private information. Fu Menglin et al. [13] This paper analyzes the security threats encountered by smart contracts, discusses the mainstream vulnerability detection methods, and finally verifies the detection effects of three symbol execution tools by experiments. Ilya Grishchenko et al.[13]The latest technologies for intelligent contract verification including formal semantics, security definitions and verification tools are summarized. This paper also pays attention to EtherTrust, a framework for static analysis of Ethereum intelligent contracts.

In this study, the blockchain technology is applied to the Electricity supplier trading system to establish a reliable trade traceability system. The contributions of this paper can be summarized as follows: The decentralized service system is constructed by the method of "Blockchain+IPFS+DB", which makes the data safe and reliable.Based on node4j, a node quick query service system is constructed, and the complex relationships within the supply chain are clarified.

**1 Implementation plan**

This system is based on Kadelima distributed peer-to-peer network and Ethereum,which stores and verifies the data lines of power supply chain and provides user data query service. Compared with the traditional centralized traceability system, this project adopts the architecture of "Blockchain+IPFS+DB", without a centralized server, and responds to users' data upload and data query requirements in units of nodes.The system architecture diagram is shown in Figure 1

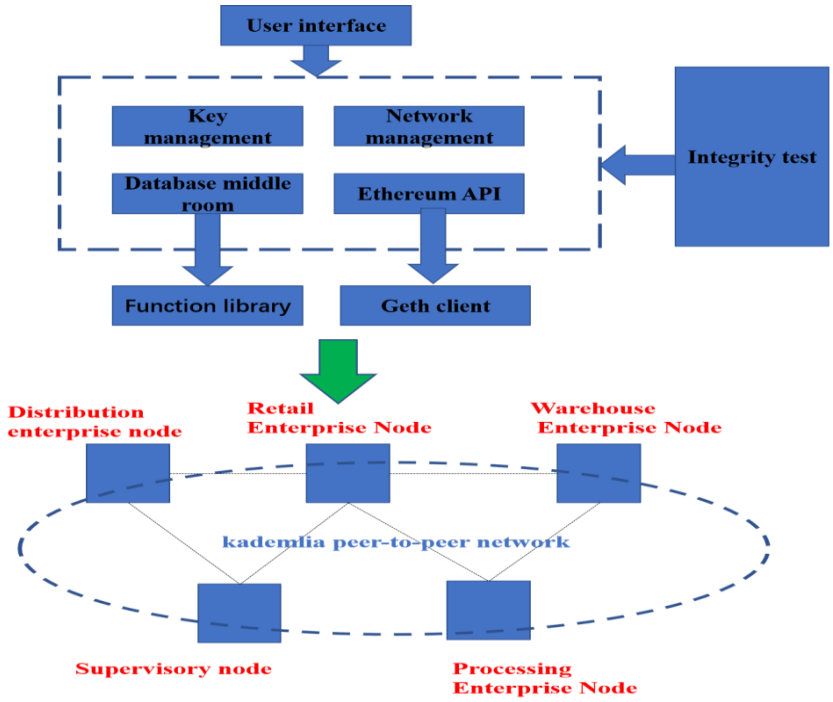


Figure 1 System framework

Firstly, the network nodes are designed. Considering the data permission requirements of different roles in the blockchain network, the system defines the following roles and permissions for different participants: (1) Data provider nodes: Data provider nodes do not join the blockchain network, but are generally enterprise nodes. If the enterprise is small,Do not have the ability to build data provider nodes, and can delegate the task of uploading data to the associated data creator nodes; If the enterprise is large in scale and has the ability to join the blockchain, it can independently become a data creation node and join the decentralized network. (2) Data viewer node: The data viewer node does not join the blockchain network.Generally, it is a consumer node or a supervision unit. The data viewer node can query the data holder data in the blockchain network through the user interaction module established by the system, and trace the source of the purchased product information. (3) Data-holder nodes: Data-holder nodes join the blockchain network and are generally enterprise nodes.An enterprise can join the blockchain backbone network as either a data provider node or a data holder node. As the core of the whole system, the data holder node, as a participant in the data persistence layer, jointly maintains the data storage of the whole system. Then design the switching interface:The interactive module adopts the form of RESTFUL structure, and transmits data directly through HTTP in light weight. The query of data location is submitted in JSON format through POST text. For the design of the persistence layer, firstly, there are many participants in the grain supply chain, and the amount of transaction data is very large, so it will be a very large expense to store all of them in the

blockchain.Additional databases are needed for secondary storage. Considering which database to use for auxiliary storage, there are the following options: relational database and non-relational database (such as file storage, key-value storage, etc.), but they can not provide a good support for the interconnected data of supply chain. Secondly,It can be seen that the traceability data of grain supply chain: products, participants, locations and events are interrelated. Taking products, participants, locations and events as nodes, and binding different entities by edges with directions can easily construct complex relationships within the supply chain.However, node4j graph database can regard relational information as the first-class entity of information storage, and the built-in optimized graph algorithm can provide high-performance fast traversal, and it is flexible in data model creation, and the operation cost of graph expansion and modification is low. Therefore, in this project, node4j database is used to store additional information besides key uplink information.Then blockchain module design: This project uses geth client of Ethereum to carry out Ethereum virtual machine environment, and uses intelligent contract to store, update and query traceability data fingerprint. The user module can access the Ethereum client through web3.js, and can use web3.js to compile, publish and call the contract.Data-holder nodes form a blockchain network through the admin.addPeer () method provided by Ethereum. Design of data integrity module: Using remote data integrity detection algorithm, the integrity and consistency of data uploaded by data providers are checked. When the data check fails, the error can be fed back to the user interaction module through the Node service module.After the data check is passed, the Node service module can further perform data persistence operation and store the encrypted hash value (data fingerprint) of the data into the blockchain node.

**2 Conclusion**

In this paper, a framework for establishing a reliable and safe Electricity trading system is proposed. Based on blockchain technology, the network nodes, interactive interfaces, blockchain modules and data integrity modules are designed respectively. For the network nodes, the relevant permission requirements are defined by different roles. In terms of interactive interfaces, the RESTFUL structure is adopted.Data can be directly transmitted via HTTP, and in terms of blockchain template design, blockchain network can be assembled by the method provided by Ethereum. In the aspect of data integrity module design, the Node service module is adopted to further store the data persistent operation in the blockchain nodes, which improves the security and query convenience.

**References**

[1] Ma ang, pan Xiao, allen wu, et al. summary of blockchain technology foundation and

application research [J]. information security research, 2017, 3(11): 968-980.

**[2]** Fu Yi, Wen Jin, Chen Huahui, et al. Review of research on blockchain for spatio-temporal data [J]. Computer Engineering, 2020, 46(3): 1-10.

[3] Zeng Shiqin, Huo Ru, Huang Tao, et al. Summary of blockchain technology research: principle, progress and application [J]. Journal on Communications, 2020.

[4] Dwork C, Naor M. Pricing via processing or combatting junk mail[C]//Annual international cryptology conference. Springer, Berlin, Heidelberg, 1992: 139-147.

**[5]** Larimer D. Transactions as proof-of-stake[J]. Nov-2013, 2013.

[6] Shirasawa K, Isuzugawa K, Ikenaga M, et al. The genome sequence of sweet cherry (Prunus avium) for use in genomics-assisted breeding[J]. DNA Research, 2017, 24(5): 499-508.

[7] Zhou L, Wang L, Sun Y, et al. Loamit: A Blockchain-based Residual Loanable-limit Query System[J]. IACR Cryptol. ePrint Arch., 2018, 2018: 655.

[8] Sompolinsky Y, Zohar A. Phantom[J]. IACR Cryptology ePrint Archive, Report 2018/104, 2018.

[9] Androulaki E, Karame G O, Roeschlin M, et al. Evaluating user privacy in bitcoin[C]//International conference on financial cryptography and data security. Springer, Berlin, Heidelberg, 2013: 34-51.

[10] Monaco J V. Identifying bitcoin users by transaction behavior[C]//Biometric and Surveillance Technology for Human and Activity Identification XII. International Society for Optics and Photonics, 2015, 9457: 945704.

[11] Fan Jili, Li Xiaohua, Nie Tiezheng, et al. Summary of smart contract technology in blockchain system [J]. Computer Science, 2019, 46(11): 1-10.

[12] Shen Xin, Pei Qingqi, Liu Xuefeng. Summary of blockchain technology [J]. Journal of Network and Information Security, 2016, 2(11): 11-20.

[13] Grishchenko I, Maffei M, Schneidewind C. Foundations and tools for the static analysis of ethereum smart contracts[C]//International Conference on Computer Aided Verification. Springer, Cham, 2018: 51-78.

[14] Ni Yuandong, Juck Zhang, Yin Tingting. Summary of research on security vulnerabilities in smart contracts [J]. Journal of Information Security, 2020, 5(3): 78-99.