

Design of Multi-interactive Electric Trading Algorithm Based on Block Chain for Micro-grid

Yanling Sun

State Grid Shandong Electric Power
Research Institute
Jinan, Shandong, 250002, P. R. China
452796077@qq.com

Yanfeng Sun

State Grid Tianjin Jixian Electric
Power Company
Tianjin, 301900, P. R. China
Yanfeng.tianjin@126.com

Xiaohui Zhai

State Grid Shandong Electric Power
Company
Jinan, Shandong, 250001, P. R. China
xiaohui1332@163.com

Yu Xing

State Grid Shandong Electric Power
Research Institute
Jinan, Shandong, 250002, P. R. China
JilinYuxing@126.com

Yuhan He

State Grid Shandong Electric Power
Research Institute
Jinan, Shandong, 250002, P. R. China
He.yuhandal@126.com

Lin Li

State Grid Shandong Electric Power
Research Institute
Jinan, Shandong, 250002, P. R. China
Jingzhen114@126.com

Abstract—This paper presents a decentralized multilateral interactive power transaction algorithm based on block chain technology for micro-grid. The intelligent micro-grid accesses a large number of distributed new energy sources, electric vehicle terminals, energy storage devices, etc., and the user side and the power generation side exhibit multilateral interaction, which is fundamentally different from the traditional centralized power grid architecture. This paper uses the block chain framework to establish a decentralized electric transaction framework. It adopts the decentralized structure to optimize the user transaction account storage index structure, and applies the decentralized multilateral interactive power trading mechanism applicable to the micro-grid.

Keywords—Block chain, micro-grid, electric transaction

I. INTRODUCTION

With the rapid growth of electricity demand, the scale of the power grid is also expanding. The traditional power generation, super-discharge, and ultra-high-voltage long-distance transmission of thermal power, hydro-power and nuclear power have been rapidly developed. However, the shortcomings of the large power grid system, such as cost and operation difficulty, are also increasingly prominent, and it is difficult to meet the requirements of users for power safety and reliability. On the other hand, issues such as the gradual depletion of global non-renewable energy sources and environmental pollution have also received increasing attention. Based on this, environmentally-friendly, reliable, flexible and efficient distributed power sources are gradually favored, which can effectively reduce system network loss, improve power factor and delay system construction update speed. In order to solve the problem of access to distributed power and large power grids, the concept of micro-grid has been proposed. The micro-grid is a special form of grid that provides electrical energy and thermal energy to nearby loads through an optimized configuration of local distributed micro-power supplies or small and medium-sized conventional power generation methods.

The micro-grid is generally built on the low-voltage side of the distribution network. The load can absorb the power generated by the distributed power source in situ, shortening the distance of the transmission line and reducing the line loss. At the same time, the micro-grid energy supply system

can also meet various needs of heating, refrigeration, humidity control, etc., effectively improving energy efficiency.

In the micro-grid mode, the sale of the main body of the electric side will inevitably show a diversified trend, and more and more independent, scattered and self-interested nodes will participate in the power market competition. How to operate the micro-grid efficiently and establish a competitive multi-user trading mechanism is one of the research priorities of the future micro-grid.

The management of power trading has two schemes for the voluntary management of central institutions and market members. The method of adopting central organization management has the following defects: a) The central organization needs to employ a large number of personnel to maintain the central database. In the process of transaction clearing, it is necessary to conduct frequent proofreading with third-party financial institutions such as banks, and the cost is high. b) From an information security point of view, once the central organization is attacked, data may be lost or tampered with, with serious consequences. In addition, excessive centralization leads to asymmetry, the central organization grasps all the transaction information of the market, user privacy is difficult to guarantee, and there may be situations in which the use of central power to harm the interests of the participants.

This paper proposes the use of block-chain technology to allow market participants to manage transactions spontaneously [1]. Block-chain technology is a distributed storage ledger. Each block is equivalent to a page in the ledger, recording the transaction information for a period of time and the hash value of the previous block. The blocks are connected in chronological order to form a block-chain. The block-chain is recorded in all nodes in the network and is maintained by all nodes. In a block-chain network, every transaction is traceable and difficult to tamper with. Therefore, when the transaction is conducted by both parties, the transaction record can be checked to verify whether the transaction can be achieved [2]. In addition, the introduction of smart contracts based on the block-chain can extend the function of the block-chain. The parties to the transaction can store the agreed agreement in the block-chain in the form of code. When the contract execution time comes, the smart

contract will be automatically executed according to the prior agreement, and the value conversion will be completed, thus solving the trust between the two parties. problem. Since the transaction is recorded in each node, when some nodes are attacked, the attacked node can reconstruct the data through the node that has not received the attack to ensure data security.

II. OVERALL FRAMEWORK OF THE TRANSACTION MODEL

A. Block-chain Data Layer Structure

This paper establishes a distributed computing platform based on public chain as the underlying framework to realize the multilateral intelligent trading of micro-grid. It consists of a smart contract layer, an incentive layer, a consensus layer, a network layer, and a data layer [3]. The intelligent contract layer can be said to be specially designed for micro-grid trading. The intelligent contract layer encapsulates a scripting language that can execute Turing. It can be deployed to the software platform by writing a scripting language as a smart contract to decentralized the application.

The data structure of the block is shown in Fig. 1. A block is divided into two parts: a block header and a block body. All transaction related information is included in the block body, and the block header contains the hash value, time stamp, random number, difficulty coefficient of the previous block and the Merkle root hash value in the block. The time-stamp is the generation time of the block, the random number is the solution of the mathematical problem, the difficulty coefficient can dynamically adjust the difficulty of the mathematical problem, and the Merkle tree is the unique identifier of the transaction in the block [4]. These constituent elements form a hash value of the block by a certain hash algorithm, and the blocks correspond to each other through the parent-hash in the block and the hash value of the previous block in the block, and are connected end to end to form a chain. Structure, and the longest chain formed from the beginning of the creation block is called the main chain. In the process of adding blocks one by one to the block-chain, it is often the case that multiple new blocks are added to the main chain to generate branches at the same time due to network delay [5]. Here, it is necessary to compare the difficulty coefficients to the entire chain. The branch with the largest cumulative workload is used as the main chain, and the process of adding blocks is continued. The time stamp in the block header guarantees the order of the block and has certain preventive effect on tampering or forging block data. The difficulty coefficient is used to dynamically adjust the difficulty of mining, to maintain the block time to float up and down in the expected time, and the difficulty coefficient is the verification basis for the proof of workload.

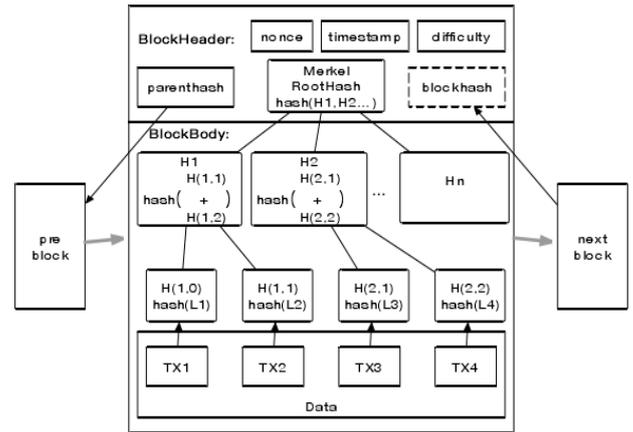


Fig. 1. Block-chain data structure.

B. Account Encryption and Signature Authentication

The security of power trading accounts mainly depends on digital signatures and asymmetric encryption algorithms. The transaction system encrypts and decrypts data through public and private keys. An account is first encrypted by the private key and sent to the public network. Only the corresponding public key can be decrypted to ensure the security of the information [6]. The chockablock built with Merkle as the data structure is to build mutual trust between nodes in this way. The signature verification process for the account is shown in Fig. 2. When other users receive the message 2 sent by B, they first find the public key of B through the address of B, and then use B. The public key decrypts the message 2, and then connects the content of the message 1 with the public key of C. The hash calculation is compared with the decrypted result. If the same, the message is considered to be sent by B. The trading system is using this technology to achieve the secret process of the message.

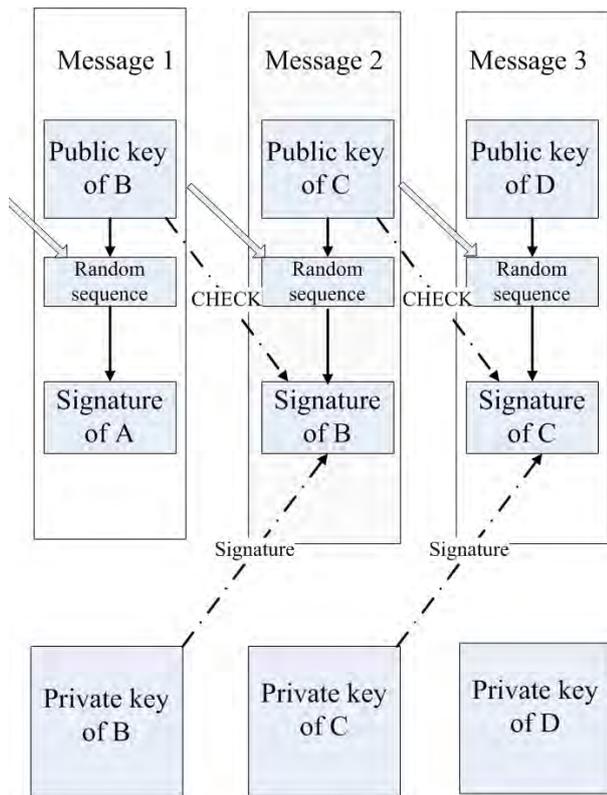


Fig. 2. Account encryption and signature authentication process.

C. Data Dissemination Mechanism

Due to the decentralized nature of the power market transaction block-chain, its network structure adopts a flat topology and uses P2P wide area broadcasting for data stream transmission [7]. In the transmission process, the various participants of the power market (hereinafter referred to as nodes) have the same status and do not have a centralized server. Each node is equivalent to participate in the routing, verification, broadcast and other functions in the system. The P2P network architecture is the network foundation for the decentralization of the power transaction block-chain. A typical P2P network topology is shown in Fig. 3.

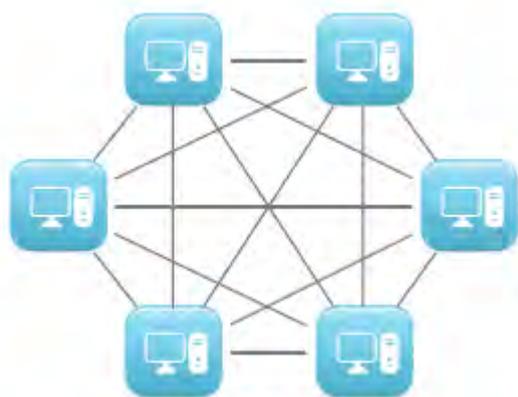


Fig. 3. A P2P network topology

When a node receives a transaction or a generated block, it sends a message to other nodes on the entire network in the form of a broadcast. Because the P2P network architecture is adopted, it is not guaranteed that all nodes receive the message when the message is broadcast. At this time, the node can send a data request request to the neighboring node, and the neighboring node sends the data for synchronization. At the same time, the network layer also includes a data verification mechanism [8]. When the node receives the information transmitted by the neighboring node, it checks the validity of the data, and the effective information broadcasts the information to the neighboring node to implement the whole network. The message is synchronized, and for invalid information, the node does not perform data forwarding operations. The power trading block-chain model uses the P2P mechanism to implement the decentralized architecture of the distributed network, making the entire network highly autonomous and reliable.

D. Consensus mechanism

In a highly autonomous decentralized distributed system, how to make the consensus of each node is the core content of the power trading block-chain. This paper adopts a consensus mechanism based on Proof of Workload (PoW), which allows a system with decentralized decision-making power to reach an agreement. Each node competes to solve a mathematical problem through computing power, and rewards the first solved node, thus promoting the computing competency of the entire network.

III. TRANSACTION ALGORITHM DESIGN

A. Transaction Block-chain Model

Each node (participant) in the block-chain has a unified block-chain client installed that can record information and communicate with other nodes. For direct power generation and power users, the client will also be associated with its smart meter to automatically record its outgoing electricity data on the block-chain. First, the power trader completes the transaction through the game, records it in the form of a smart contract, and spreads it to each node of the entire network through the P2P network. Through the communication, each node of the whole network forms a consensus on the concluded transaction. Next, distributed security checks are performed on temporary transactions by market participants. If the security check is passed, the transaction will be recorded on the block-chain. If the transaction does not meet the security check, the market participants re-game to complete the transaction, and re-check the security, after repeated iterations, finally reach the transaction that meets the line trend constraints, and record the transaction on the block-chain. In the distributed micro-grid, a complete transaction algorithm flow is shown in Fig. 4.

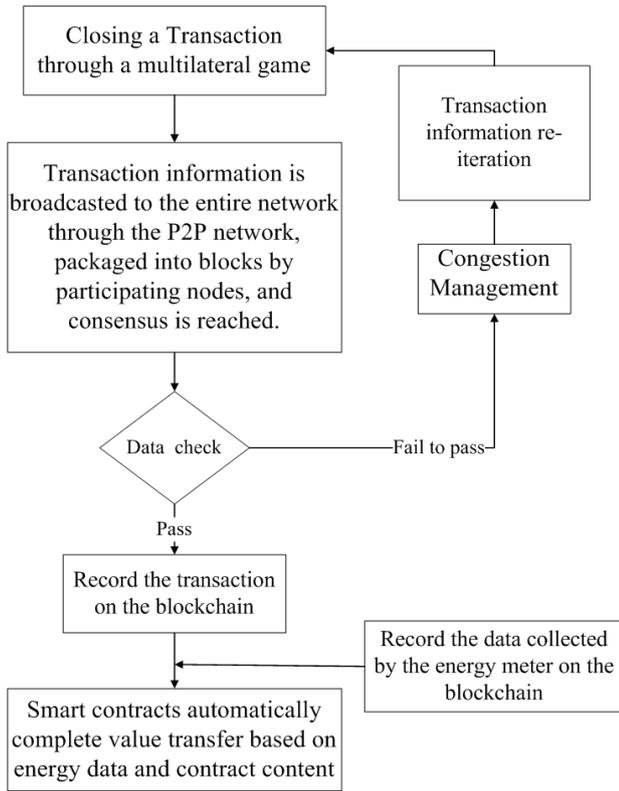


Fig. 4. Block-chain-based micro-grid trading algorithm model.

When a node receives a transaction or a generated block, it sends a message to other nodes on the entire network in the form of a broadcast. Because the P2P network architecture is adopted, it is not guaranteed that all nodes receive the message when the message is broadcast. At this time, the node can send a data request request to the neighboring node, and the neighboring node sends the data for synchronization. At the same time, the network layer also includes a data verification mechanism. When the node receives the information transmitted by the neighboring node, it checks the validity of the data, and the effective information broadcasts the information to the neighboring node to implement the whole network. The message is synchronized, and for invalid information, the node does not perform data forwarding operations. The power trading block-chain model uses the P2P mechanism to implement the decentralized architecture of the distributed network, making the entire network highly autonomous and reliable.

B. Consensus mechanism algorithm

In a trading system with n nodes, the primary node is responsible for generating new blocks. When all nodes have negotiated and verified the block, a consensus is reached on the block. Each node takes the same order at initialization. Each node establishes inter-node communication according to the IP address in the configuration file. After establishing communication, it will send the corresponding public key to other nodes. Other nodes complete the verification by private key signature. The verification indicates that an effective connection is established between the nodes. During the negotiation process, there are three states for a message node: Pre-prepare, Prepare, and Commit, respectively, represented by $P1i\{d,m,n\}$, $P2i\{d,m,n\}$, $P3i\{d,m,n\}$. Where d is the

number, m is the certificate message, n is the number of the sending certificate message node, i is the number of the current node, and the consensus algorithm is as follows.

Input: certificate message

Output: whether or not reach consensus.

Repeat

If (m ≠ key) then

If (state = P1i {d,m,n})

If (i = d mod N) then

Send P1i certificate to other

State == P2i {d,m,n}

Else

State ==P2i {d,m,n}

If (state =P2i {d,m,n})

Send P2i certificate to other

If (Num (m) > (2/3) N) then

State == P3i {d,m,n}

Else

State ==P2i {d,m,n}

If (state =P3i {d,m,n})

Send P3i certificate to other

If (Num (m) > (2/3) N) then

Verify the certificate

Return true

Else

State ==P2i {d,m,n}

Until d changed

When a certificate is generated, it first determines the state of the node and performs the current state. When a certificate is judged by three conditions, the content of the certificate is considered to be a consensus among the nodes.

C. Block Generation ,Execution and Check

This paper uses the transaction verification protocol to generate new blocks. After the self-node first checks the validity of the transaction, the transaction is batch-written into the block, and the block is sent. The transaction in the block passes through other nodes of the whole network and is added to the block-chain, and the transaction is considered carried out. When the transaction arrives, the master writes the transaction to the block and broadcasts the block. After the network node agrees on the block, it tries to add the block to the block-chain. The whole process is asynchronous, and the order of the block is guaranteed by the block number and the hash value of the parent block recorded by the block.

Fig. 5 shows the execution of a normal request by a system consisting of 4 nodes. As can be seen from Fig. 5, a

consensus and implementation of a message needs to be agreed upon after three phases of implementation negotiation.

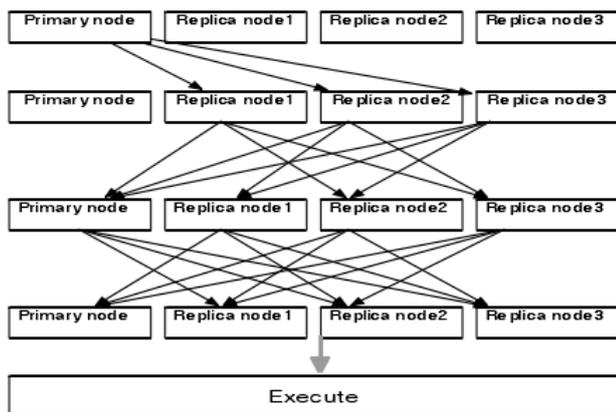


Fig. 5. Execution process of a four nodes transaction system.

The block check process is mainly for verifying the block header information. Transaction check is the core content of the entire block-chain check. We define the state trade function W , the transaction is T , the execution of the transaction will change the local state database, here the database state is defined as S , then there is.

$$S' = W(S, T) \quad (1)$$

Where S' is the new state after the change, a valid transaction should satisfy the following conditional equation.

$$s(T) \neq \phi \wedge S[s(T)] \neq \phi \wedge T_n = S[s(T)]_{nonce} \wedge v_o \quad (2)$$

Where $s(T)$ is the originator of a transaction, T_n is the *nonce* and transaction amount in the transaction, and *nonce* is the number of transactions recorded in each account to ensure the order of the transaction and recorded in the account. Information.

IV. CONCLUSION

In the smart micro-grid environment, the access of a large number of energy producers will generate new business models, with point-to-point bilateral transactions of energy. This paper proposes a method for managing power transactions using block-chains. Using a decentralized

architecture, the block-chain and smart contract technology are used to enable the entire network node to maintain and manage transaction information and automatically transfer funds. This paper introduces the basic framework of the power market trading block-chain, data encryption, decryption and signature mechanisms, information dissemination methods and consensus-building principles. Finally, this paper proposes a logical model of block-chain trading in the electricity market, a consensus algorithm based on the Byzantine mechanism and block generation, execution and security check algorithms. Although this paper focuses on the application of block-chain in micro-grid structure power trading, this approach can be similarly extended to other energy sources such as natural gas and thermal energy. Each account in the block-chain can manage multiple energy sources, and transaction information of different energy sources is recorded in the block-chain at the same time to realize the interconnection of energy transactions.

REFERENCES

- [1] M. Alam, H. Li, and A. Patidar, "Bitcoin for smart trading in smart grid," The 21st IEEE International Workshop on Local and Metropolitan Area Networks, China, pp. 1-2, 2015.
- [2] Y. Yang, J.H. Zhao, and F.S. Wen, "Blockchain in Energy Systems: Concept, Application and Prospect," Electric Power Construction, vol. 38, issue 2, pp. 12-20, 2017.
- [3] N. Zhang, Y. Wang, and C.Q. Kang, "Blockchain Technique in the Energy Internet: Preliminary Research Framework and Typical Applications," Proceedings of the CSEE, vol. 36, issue 15, pp. 4011-4022, 2016.
- [4] A. Thomson, T. Diamond, S. Weng, K. Ren, P. Shao, and D. J. Abadi, "Calvin: Fast distributed transactions for partitioned database systems," ACM Int. Conf. Manag. Data, pp. 1-12, 2012.
- [5] E. B. Sasson, "Decentralized anonymous payments from bitcoin," in Proceedings. IEEE. Security Privacy, pp. 459-474, 2014.
- [6] E. Gaetani, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, "Blockchain-based database to ensure data integrity in cloud computing environments," In ITA-SEC, volume 1816, 2017.
- [7] G. Zyskind, O. Nathan, and AS Pentland, "Decentralizing privacy: using blockchain to protect personal data," 2015 IEEE Security and Privacy Workshops. San Jose, CA, pp. 180-184, 2015.
- [8] S. Omohundro, "Cryptocurrencies, smart contracts, and artificial intelligence," AI matters, 1(2): 19-21, 2014.