Research and Prospect of Key Technologies in Power Trading Blockchain

Lei WANG$^{1,2}$, Hai-ning WANG$^{1,2}$, Ying-fei CHAO$^{2,*}$, Shu-hong SHI$^{1,2}$ and Pei-yu XI$^{1,2}$

$^1$Nari Group Corporation/State Grid Electric Power Research Institute Nanjing 210003, China
$^2$Beijing Kedong Electric Power Control System Co., Ltd. Beijing 100194, China
$^*$Corresponding author

Keywords: Blockchain, Power trading, Information security, Consensus mechanism.

Abstract. This paper discussed the application of blockchain technology in power trading business, and focused on solving the information security problems which currently faced by power trading, including protecting the privacy of market entities, encrypting key data. This paper proposes the idea of controlling user access through CA nodes, using zero-knowledge proof mechanism to protect user privacy, and adopting pluggable way to set consensus mechanism. This paper proposes an innovative vision for building a power trading blockchain, providing advice for future power trading blockchains.

Introduction

The development of blockchain technology around the world is in the ascendant. It has experienced three stages of development [1]: Bitcoin has emerged in the blockchain 1.0 digital currency era, initially realizing the idea of decentralization of currency transactions; blockchain 2.0, the concept of smart contract is proposed. The two parties agree on the contract content and automatically trigger the contract execution when certain conditions are met. The blockchain 3.0 develops distributed artificial intelligence and organization on the basis of 1.0 and 2.0, giving full play to its network self-organization. The characteristics of distributed mutual trust, the application of technology is no longer limited to the economic field, and gradually began to infiltrate all walks of life, including the field of electricity market transactions. At present, in New York, USA and Busselton, Australia, energy trading systems based on blockchain technology are put into operation [2-3].

In October 2016, the Ministry of Industry and Information Technology issued the “White Paper on China's Blockchain Technology and Application”, proposing relevant suggestions for blockchain technology and application development, and promoting the development of China's blockchain technology and industry. Up to now, the application of domestic blockchain technology has emerged in industries such as insurance, finance, and electronic deposit certificates. The issuance and implementation of the "Opinions of the Central Committee of the Communist Party of China and the State Council on Further Deepening the Reform of the Power System” (Mid. 9) in March 2015 marked the beginning of a comprehensive deployment of the new round of power system reform in China [4]. The market for electricity-selling side is gradually opening up, the number and variety of power trading entities are increasing, the volume of trading business is increasing, and the interconnection and inter-operating services among multi-level markets are more frequent. The blockchain technology based on P2P network will have the opportunity to become a new generation of power trading platform. Foundation.

By analyzing the characteristics of power trading business and blockchain technology, this paper proposes the feasibility of constructing a power trading blockchain, and puts forward constructive opinions on key issues such as information security protection.
Power Trading Business and Blockchain

Blockchain technology has the main features of decentralization, consensus mechanism, traceability, etc. [5-6], which can solve some problems in the power trading business.

1) Decentralization

Traditional power trading is based on the power trading center, and each node in the blockchain is the center. In other words, each node is equal, and some nodes have problems that will not affect the operation of the entire system. With the gradual liberalization of the power-selling market in China, the number, types, and types of business involved in the transaction are gradually increasing. If a centralized control method is still adopted, the power trading center will invest a lot of manpower and resources, and it is difficult to achieve low cost. Large-scale participation in user interaction. Once the centralized node trading center has uncontrollable problems, such as data being tampered with, the server is paralyzed, the entire network system will be affected, causing serious transaction accidents and triggering a crisis of trust. The blockchain is transmitted point-to-point. It does not rely on any single node. Any single member to modify the information will not be recognized by other market members. Therefore, after the traditional centralized trading method is transformed into a distributed trading method based on blockchain, the market will no longer need to rely on the trading center to control, and each transaction is recorded and stored in a distributed form. In the chain, the status of each market entity is equal, and jointly maintaining the normal power trading will help ensure fair and fair transaction data, and power trading will have higher security and reliability.

2) Consensus mechanism

All participating market users in the power trading blockchain network jointly determine the validity of a transaction information through POW (Proof of Work)\POS (Proof of Stake)\DPOS (Delegated Proof of Stake)\FBET (Practical Byzantine Fault Tolerance). The consensus algorithm ensures that the content recorded in each block is consistent, ensuring the authenticity of the information. In the blockchain application, there is no need to rely on the trading center to identify and verify whether a transaction is established. Only when more than 51% of the market members reach a consensus, the transaction can occur, which can effectively reduce the occurrence of counterfeit transactions and thus achieve balance between efficiency and security.

3) Traceable

The transaction records of the traditional power trading business rely on manual recording, and a large amount of data is recorded in the EXCEL table, which is prone to operational errors and loss. The power transaction data information in the blockchain is stored in a time-stamped chain block structure, ensuring that once the transaction record is created on the block, it is almost impossible to change, with strong traceability and verifiable. Any two blocks in the blockchain are associated by cryptographic methods and can be traced back to the data of any block. The blockchain technology adopts the distributed general ledger accounting method, which can not only solve the problem of false accounting and error accounting in the automatic demand response business, but also establish a complete traceable transaction system for each participating transaction fund (such as: special subsidies for renewable energy power generation, contractual breach of fines, etc.) for the settlement of the settlement, when a transaction dispute occurs, can be found to be evidence.

Key Technology of Power Trading Blockchain

In order to realize the application of blockchain technology in the field of power trading, there are still many key issues to be solved urgently. This paper selects information security and consensus mechanism to explore and hope to provide some reference for the construction of the future power trading blockchain.

Information Security Issue

Blockchain technology adopts P2P distributed storage technology, and each node records all transaction data through a consensus mechanism. The power trading platform based on blockchain
technology must follow this feature, and cannot use the centralized storage information protection method. Therefore, the protection of transaction information security will face new challenges.

Combining the characteristics of general electronic transactions with the particularity of the power industry, the following basic requirements are imposed on the information security of power trading systems: each subject in the trading system is an authorized user who must undergo strict examination, not a general public user, mainly including various power generation companies, grid companies and large users etc. [7]; For the data required for confidentiality, the data is encrypted and encrypted, and the authenticity, integrity and accuracy of the transaction data are guaranteed.

At present, the power trading system uses the user name + password mechanism to authenticate the internal and external customers of the power company. Due to the password of this type of authentication is transmitted in plain text on the network, and the password still has insecure factors such as being easily guessed, violently attacked, intercepted by the network, and leaked from the server, the lack of a secure and effective access control mechanism for user passwords on the server side is likely to cause data theft and destruction [8]. The traditional power trading platform, one is to control the access rights by using the internal network to separate the access; the second is to store the data to be protected (including the power transaction results, the declaration data) in the centralized node, usually the server of the transaction center. It is stored in the database through encryption technology to ensure that the data address that needs privacy protection cannot be accurately accessed, and that no leakage occurs during data transmission, which means that it cannot be effectively monitored by the intruder.

In order to build a power trading blockchain, this paper proposes a new CA node to implement PKI services and restrict access rights; by using zero-knowledge proof (ZKPs) technology to address two challenges that the inferred transaction address attribution and visible transaction amount which power trading platforms are facing in the privacy protection.

**Restricted Permissions.** Due to the underlying design of the blockchain technology, any node in the public chain such as Bitcoin or Ethereum can join the network without permission, stealing communication information in the network, and the security is low. All members of the Internet are not required to join the chain in the power transaction. Therefore, it is more appropriate to select a partial decentralized alliance chain as the power trading blockchain.

Inspired by the typical super-logger-Fabric of the alliance chain, the power trading blockchain uses the power trading center server as a CA (certificate authority) node. All market members in the power trading blockchain must be certified by the power trading center to access the network. The CA node implements the PKI (Public Key Infrastructure) service and is mainly responsible for managing identity certificates, including generation and revocation. The trading center can issue an identity certificate in advance and send it to the corresponding market members. After deploying the certificate, these market members can access various resources in the network. During the follow-up visit, members do not need to make a request to the power trading center again. Therefore, the processing process of the CA node is completely decoupled from the processing of transactions in the network. After issuing the certificate, the power trading center does not participate in the transaction process in the network, and does not cause any performance bottleneck [9].

The power trading blockchain will adopt a digital certificate mechanism to realize identity authentication and authority control. Digital certificates, also known as "digital ID cards" and "network ID cards" are electronic documents that are issued by CA and digitally signed by CA, containing information about the public key owner and public key. It can be used to identify the identity of a market member who has a digital certificate. The digital certificate contains the public key, certificate name information, the digital signature of the issuing authority for the certificate, and the matching private key. When a transaction is generated, the sender encrypts the data using the recipient's public key, and the recipient decrypts it using its own private key. At the same time, the sender digitally signs the sent message digest with its own private key to confirm whether the identity of the sender and the content of the verification information have been tampered with, and enhance
the sender's non-repudiation of the transmitted information [10]. Considering factors such as anti-aggression, calculation and processing speed, ECC (Elliptic Curves Cryptography) should be used for such asymmetric encryption. The certificate can be stored in a database in the network. When the certificate is revoked, the CA that issued the certificate still retains a copy of the certificate in case the dispute may be resolved in the future.

**Data Encryption.** In the power trading business, before the transaction is completed, it is usually necessary to protect the source, destination and transaction content of the transaction, that is, the transaction parties are anonymous and the transaction data is not visible. This is a problem in applying blockchain technology to power trading.

In addition to using hash functions and asymmetric cryptography, a variety of cryptographic algorithms and techniques that are maturely applied to blockchains can ensure that transactions can be safely carried out in the case of decentralization. This paper proposes the idea of applying zero-knowledge proofs (ZKPs) to the power trading blockchain. The concept of zero-knowledge proof (ZKPs) was first proposed in the 1985 "Intellectual Complexity of Interactive Proof System". Zero-knowledge proof is a way to prove certain data operations without revealing the data itself. This method allows both parties (the prover and the verifier) to prove that a proposal is true and does not need to disclose any information other than "it is true." In cryptographic currency and blockchain, this usually means that the transaction data can be verified to be true without knowing any other information.

Zcash is the first blockchain system that uses a zero-knowledge proof mechanism and is currently the best digital currency for privacy protection [11]. Zcash provides full payment confidentiality, which uses a commitment function to encapsulate the value of the sender, payee, and even the transaction of each transaction into several parameters. At the same time, the zero-knowledge proof technology zk-snarks is used to prove the transaction, and the proof process does not need to disclose relevant information, so the blockchain transaction can be hidden. Only users with the correct view key can view the contents of the transaction. Users have full control and can choose whether to provide viewing keys to others. However, the process of generating proof by the zk-snarks algorithm is very slow, usually takes 1 minute to generate a new proof, and there is a bottleneck in efficiency. How to improve the efficiency of the market members on the premise of ensuring the privacy of market members remains to be solved.

**Consensus Mechanism**

The blockchain consensus mechanism is used to verify the validity of each record, thereby preventing arbitrary nodes from tampering with data [12]. The power trading platform based on blockchain technology and the traditional power trading platform guarantee data, the biggest difference in database consistency selection is which node becomes the node initiated by the checkpoint. Because the database adopts the master-slave mechanism, the master node is always the originating node of the log, and the slave node is always the log playback and verification node. However, the blockchain uses certain algorithms (such as PoW, PoS, DPoS, etc.) to periodically select a node between multiple participating nodes for checkpoint confirmation. The consensus algorithm can also ensure that transactions are not forged and falsified. This is also a reason for the blockchain to claim its own security: in a large number of nodes across the network, the attacker cannot determine who the node is confirmed by the next checkpoint (Even if the attacker determines the next block node, it can still pass digital signatures and other techniques).

Different consensus mechanisms affect the consistency, performance, throughput, and reliability of the blockchain. At present, the consensus mechanism mainly includes the PoW (Proof of Work), PoS (Proof of Stake), DPoS (Delegated Proof of Stake), FBET (Practical Byzantine Fault Tolerance) which have been maturely applied and Casper, PoET (Proof of Elapsed Time), etc., that to be further studied.

At the consensus level, a consensus mechanism can be set up according to specific needs in a pluggable manner [13]. At present, it tends to select the PBFT Byzantine algorithm that has been matured. PBFT does not need bitcoin or other types of tokens, and achieves a 33% fault tolerance rate,
which can well adapt to the needs of the power trading alliance chain. PBFT does not protect against
witch attacks and is not suitable for public chains. POS and DPOS require token participation and are
not suitable for industrial applications.

PBFT has better fault tolerance, but after the introduction of the CA certification system, each node
has access control, and the demand for fault tolerance in the more secure and stable alliance chain is
not very strong. To improve transaction performance, you can choose to sacrifice partial fault
tolerance to improve concurrency and transaction performance. For this reason, Hyperledger 1.0
chose to use Kafka to replace PBFT in version 0.6.

Table 1. Consensus mechanism comparison.

|                  | PoW | PoS  | DPoS | PBFT | Casper | PoET |
|------------------|-----|------|------|------|--------|------|
| Performance      | Lower| Low  | High | Higher| High   | Higher|
| Degree of
decentralization | complete| complete | complete | Semi-centralized | complete | Semi-centralized |
| Maximum number of allowed nodes | 51% | 51% | 51% | 33% | 51% | 51% |
| The need for
tokens          | YES | YES  | YES  | NO   | YES    | NO   |
| App types       | Public chain | Public chain | Public chain | Alliance chain | Public chain | Alliance chain |
| Guard against
deploy attacks | YES | YES  | YES  | NO   | YES    | YES  |
| Technical maturity | Mature | Mature | Mature | Mature | Not applied | Not applied |
| Requires dedicated hardware | NO | NO   | NO   | NO   | NO     | YES  |

Summary

Blockchain technology, with its decentralized nature, has a good development prospect in the power
trading business. However, in order to truly build a power trading platform based on blockchain
technology, in addition to solving information security problems, there are still other problems that
need to be solved, such as: transaction speed. Power trading emphasizes real-time performance. When
trading, it is impossible for trading members to spend dozens of minutes waiting for data encryption
and transaction confirmation.

In addition, the blockchain technology is not limited to applications in the power trading business,
but has adaptability in the power business (electric power dispatching, power marketing, power
settlement), but needs to consider the power flow problem without affecting network congestion. In
the future, it is expected to be built into a P2P power network covering all power services.

Acknowledgement

This research was financially supported by the State Grid Corporation Headquarters Science and
Technology Project.

References

[1] Zhu Xingxiong, Chen Shaozhen, He Qingsu. Microgrid System Based on Blockchain [J].
Electronic Technology and Software Engineering, 2018(01): 157-159.
[2] Rutkin A. People-powered grid [J]. New Scientist, 2016, 229(3064): 22.
[3] Rutkin A. Blockchain aids solar sales [J]. New Scientist, 2016, 231(3088): 22.
[4] Yan Yu, Li Gengyin, Li Guodong, Zhou Ming, Pang Bo, Li Zhu. Analysis of the situation of direct power trading under the new round of electricity reform [J]. China Electric Power, 2017, 50 (07): 33-37.

[5] Tan Lei, Chen Gang. Blockchain 2.0 [M]. Beijing: Publishing House of Electronics Industry, 2015.

[6] Zhang Ning, Wang Yi, Kang Chongqing, Cheng Jiangnan, He Dazhao. Blockchain Technology in Energy Internet: Research Framework and Typical Application [J]. Proceedings of the CSEE, 2016, 36(15): 4011-4023.

[7] SUN Hanyan, Liu Dong. Information Security Strategy for Electricity Market Trading Based on Time-Space Model [J]. East China Electric Power, 2006(05):1-5.

[8] Yu Yong, Lin Weimin, He Jun. Design and Application of Power Digital Certificate Service System [J]. Automation of Electric Power Systems, 2005(10): 64-68.

[9] Superbook Fabric's architecture and design [J]. Computer Programming Skills and Maintenance, 2017 (18): 4-5.

[10] Zheng Junting, Rao Wenjun, Wan Dazhao. Discussion on the working principle and application of digital certificate [J]. Enterprise Science and Technology and Development, 2010(18): 32-34.

[11] Zhu Lihuang, Gao Feng, Shen Meng, Li Yandong, Zheng Baokun, Mao Hongliang, Wu Zhen. A Review of Research on Blockchain Privacy Protection [J]. Computer Research and Development, 2017, 54(10): 2170-2186.

[12] Li Jia. The Best Practical Technology of Value Internet Blockchain—Information Security [J]. Computer and Network, 2018, 44(04):53.

[13] Tang Wenjian. How the blockchain will redefine the world [M]. Mechanical Industry Press, 2016.