Research on Zero-trust Security Protection Technology of Power IoT based on Blockchain

Zhiyu Chen¹*, Longchuan Yan¹, Zitong Lü², Yanling Zhang³, Yonghe Guo¹, Wenjing Liu¹, Jiaxing Xuan²

¹State Grid Information & Telecommunication Branch, Beijing, China
²State Grid Electronic Commerce Co., Ltd., Beijing, China
³China Electric Power Research Institute, Beijing, China
*Corresponding author’s email: sevsevf@163.com

Abstract. With the access of massive terminals in the power Internet of things (IoT), the efficiency of information sharing is improved, but the grid boundary is increasingly blurred. The traditional centralized security management mode is facing a severe security situation, which is difficult to meet the high security requirements of the system operation. There are three main risks: 1) the execution authority of control information is not strictly controlled at the equipment level; 2) Data and authority are not separated, which makes the security management of data layer have hidden dangers; 3) Power supply chain is faced with the problems of data island, data trust and performance guarantee. Based on the characteristics of blockchain technology (BcT), such as non-tampering, collective maintenance and transaction non-repudiation, this paper constructs a data protection architecture covering device layer, data layer and business layer, realizes high-level security protection of data flow in all links of power network, and improves the security management and control ability of the system. Through the scheme proposed in this paper, the implementation of control information is strictly managed, the use rights management of data is more standardized, and the credibility and interaction rate of business data are greatly improved.

Keywords. Zero-trust, blockchain, power IoT, security protection

1. Introduction

As the country's key infrastructure, the scope of power system services involves all walks of life. The safe and stable operation of power services is related to national security, so it has become a key focus. As my country's industrial and residential electricity load continues to grow rapidly, the power system must meet the ever-increasing demand for power supply. With the transition of smart grid to energy Internet, the changes in the grid load, form of the power system must comply with safety, compatibility and robustness. Correspondingly, the risks faced by the circulation of data in all aspects of the system are also increasing day by day [1].

Modern information and communication technologies such as cloud computing, blockchain, big data, IoT, and artificial intelligence have realized multi-dimensional extensions and information interaction from power networks to people, things, and locations. With the access of a large number of business terminals, fragmented operation data is collected by different sensing devices and provided to data center for management analysis, which greatly improves the timeliness of data interaction.
between internal and external networks of the enterprise, and realizes generation, transmission, transformation, and distribution. Data integration in various links such as electricity and electricity consumption. However, while the openness of the Energy Internet has improved system operation efficiency, trust issues in various links have gradually become prominent, and new risks and vulnerabilities have also increased. The legal access and security management of business terminals are facing severe situations. The traditional technology of network security protection still have some limitations. Traditional border-based network security is based on a partitioned and layered model, using firewalls, WAF, IPS and other devices to block third-party attacks outside the border. However, most of the attacks lurked in the intranet in the early stage, and then gradually gained higher authority through system vulnerabilities or management defects. Meanwhile, human misoperations and malicious sabotage are also potential threats to network security [2]. The network security protection for the zero trust environment is gradually concerned by the society.

With the rapid development of the Energy Internet, a large amount of fragmented operation data is collected by different sensing devices and provided to the data center for management analysis, which effectively improves the synergy efficiency between the user side and the supply side. However, while the openness of the Energy Internet has improved system operation efficiency, the blurring of network boundaries has gradually highlighted the trust issues in various links, and new risks and vulnerabilities have become increasingly prominent. Legal terminal access and security management are facing severe challenges. Traditional network security technology that relies on the central organization cannot meet the high security requirements of the development of the new energy Internet business. The central node may cause data leakage or even network paralysis when management defects or attacks are encountered. In response to the security protection requirements of "generation-transmission-transformation-distribution-use" and other links, the power industry is actively conducting research on power information network security protection technology in a zero trust environment [3,4].

BcT solves the risk of network trust in a decentralized way, and realizes the secure interaction of information. The data sharing rate of each link of the existing power system is limited, and the information in business flow is difficult to be completely symmetrical and transparent, and there are risks of false information and tamper data. BcT has the characteristics of non-tampering and credible information, which can establish a credible information interaction mechanism and provide reliable support for the secure interaction of distributed data. This article combines power scenario to study the application of BcT in security protection. This technology strengthens the efficiency of information exchange between systems, reduces costs and also ensures data security.

In response to the high security requirements of the Energy Internet in terms of network identity authentication, trusted information interaction, and data privacy protection, this article combines the power information network architecture to analyse the current status of business data protection from the perspective of data security, and combines typical application scenarios to build a district based The new generation of power information security protection strategy based on blockchain technology strengthens the robustness of the power system in the complex power network environment.

2. Blockchain technology
As a new type of data sharing technology, blockchain has created a new computing paradigm and collaboration model that can establish trust at low cost in an untrusted competitive environment. With its unique trust establishment mechanism, it has achieved penetrating supervision and the trust is transferred step by step, forming a network that allows all data to be transmitted to each node when it is created, effectively avoiding third-party behavior risks. Blockchain has the characteristics of decentralization, autonomy, openness, and non-tamperability, which can effectively reduce the cost of trust between participants [5,6].

As a basic supporting technology, blockchain has good penetration, and it can be deeply integrated with emerging technologies such as big data, Internet of Things, and artificial intelligence. With its
technical characteristics of data preservation and traceability, it can further improve power information level of chemical technology and supporting capabilities. Blockchain is a decentralized database that multiple nodes participate in and maintain together. It has the characteristics of anti-counterfeiting, anti-tampering, and traceability. The information on the chain records all the information of the transaction, and forms an operating mechanism with efficient and transparent processes, high data security, and multi-party trust collaboration. It has a high compatibility with distributed energy interconnection and interaction, which is conducive to solving the equipment manufacturing in the power industry chain. Data sharing, multi-party collaboration, security and other issues, and promote the improvement of production efficiency and the reduction of operating costs. The block chain consists of two parts: a block header and a block body. The block header is composed of the version number, the hash value of the previous block, the Merkle root node, the timestamp, the difficulty value, the random number and the transaction record. Based on the characteristics of the hash encryption algorithm, if any transaction record is tampered with, the root node of the Merkle tree of the binary tree structure will inevitably change, and other nodes can clearly find the problem when verifying the hash value. The structure of the blockchain is shown in Figure 1. Multiple transactions are recorded in the block and stored in the block header in the form of a Merkle root based on Hash calculation. Each block header stores the Hash value of the previous block, forming a chain structure.

**Figure 1.** The structure diagram of blockchain

In the blockchain, the consensus mechanism is used to solve the consistency problem of information transmission and value transfer in the distributed system, and to ensure that the established operation is consistent, recognized, and non-tamperable in the distributed network. Transactions are written into the blockchain through a consensus mechanism, and relying on the multi-party mutual trust mechanism formed by the consensus algorithm, without the participation of a centralized organization, large-scale and efficient collaboration can still be completed. Because the traditional power Internet of Things management system controls and maintains equipment data and business information in the form of a centralized structure, the computational load and security issues of the central node have become important research propositions. This paper proposes to use blockchain technology to build a decentralized power IoT system, eliminate the security risks of central nodes, realize effective management of equipment identity and business data flow, and ensure the integrity and non-tampering of equipment permissions and control records.

### 3. Security protection of IoT device

With the deployment of large-scale power terminals, various network services and network entity identities have exploded. Security incidents such as fraudulent use of network identity, identity information leakage, account brute force cracking, and account authority abuse are frequent, seriously threatening the stable operation of power companies. In the ubiquitous, hybrid and wide-area interconnected environment, network security threats and risks have transcended boundaries. The traditional security infrastructure based on physical boundaries and relying on network locations to establish security trust has been completely broken. Therefore, we use authentication and authorization establish a trust foundation for a new security defense system [7].
In the traditional identity management model, the data of each unit cannot be communicated in isolation, the risk of data leakage in the centralized management system is high, and the data authentication format and security level are different [8,9]. Therefore, this article proposes to introduce blockchain into identity management to realize the unification of identity management and reduce the risk of data leakage through decentralization. Identity authentication based on BcT performs decentralized and confidential storage of the identity information of all nodes, which can effectively prevent the single-point failure and the difficulty of multi-CA trust in traditional authentication methods. At the same time, the system introduces authentication such as biometric authentication factors and dynamic passwords. Using the timestamp and random number contained in the block header of each block can effectively prevent replay attacks in the process of creating blocks and prevent attackers from cracking identity information offline. To achieve effective protection of private information.

![Figure 2. Device management based on blockchain](image)

In order to realize the trusted interaction between the power IoT devices, and the control information can only be run when the device has the execution authority, a device-level security protection architecture based on BcT is designed. Figure 2 shows the IoT device management model based on BcT. The interactive information and permissions between devices are recorded on the blockchain. In the initial stage of system operation, the system generates the required keys and initial blocks. After the user defines the strategy required, the record is uploaded to the initial block. During the operation of the system, information interaction between devices requires user authorization first, and communication or control can only be carried out after obtaining the key distributed by the system to ensure authority security and interaction privacy. The interaction information between devices is recorded and released on the blockchain in chronological order. After the device identity and execution authority are confirmed, the control information can be executed. Therefore, the security of equipment and confidentiality, integrity, and availability of data can be guaranteed.

In order to ensure the credibility of the information interaction of power IoT devices, control information can only be executed if the device has permission. In the initial stage of system operation, the system generates the required keys and initial blocks. At the same time, the system runs according to the user-defined policy and records it to the initial block. During system operation, the device needs to obtain user authorization before it can obtain the keys distributed by the system for control or communication, ensuring the security of permissions and communication privacy. After the blockchain system releases the block recording information, the identity and authority of the device are confirmed, and the control information can be executed.
4. Security protection of IoT data
In the power IoT environment, with multiple data sources, high storage complexity, and multiple application scenarios, there are very high requirements for data security. Based on the non-tamperable and traceable security features of BcT, a large amount of private data can be effectively controlled, ensuring the authenticity of information. In order to form a decentralized data and authority management model, this article applies BcT to external distributed databases to realize the separation of data and data authority [10,11]. Application systems need to be authorized to access business data.

As shown in Figure 3, the operation instructions of the operator and the application system on the data are recorded on the blockchain. The application system sends a request for access to the data and records it to the blockchain. The system checks the signature and the record of the blockchain to confirm the application system Do you have access rights to the corresponding data? If the check is passed, the operation will be recorded on the blockchain, and the database will return the data to the application system. Because the blockchain has a complete record of the behavior of the application system, the operator can change the data access authority at any time. The data manipulation process is transparent and auditable to the operator. The operator can track the data, know what kind of data is acquired by what application and by what method, to ensure data security.

Under the environment of power IoT, business data has the characteristics of wide collection channels, diverse application scenarios, complex storage structure, and so on, which has high requirements for data security. Through the combination of BcT and external distributed database, the separation of data and data authority can be realized, and the decentralized data management system can manage data and authority. The operation instructions of operators and applications for data are recorded on the blockchain. The application sends access data requests and records them to the blockchain. The system checks the signature and the records of the blockchain to confirm whether the application has access rights to the corresponding data.

5. Security protection of IoT business
The power industry is closely focusing on the energy Internet strategy and vigorously promoting the "Internet +" transformation. E-commerce, integrated energy and other businesses have developed rapidly, and the corporate supply chain is also constantly changing and extending, covering manufacturers and service providers, channel vendors, financial institutions, regulatory agencies, customers and other nodes. With the increasing difficulty of supply chain management, collaboration efficiency faces many constraints, manifested in data islands, data trust, and performance guarantees. Facing the power business scenario with multi-stakeholder participation, improving the utilization of data assets have become one of the urgent problems to be solved [12].
The blockchain-based supply chain collaborates with upstream and downstream companies to participate in transactions. Multi-party trust promotes a more real, transparent and smarter industrial ecological chain, and realizes the interconnection, credible sharing and orderly sharing of information such as digital identities and data assets. Collaboration can ensure the automatic execution of enterprise contracts in accordance with the agreed fair and independent operating mechanism. Therefore, building a power supply chain based on BcT can open up the transaction relationship between various entities, realize the transfer of credit between core enterprises and remote enterprises, and expand the service scope of supply chain finance [13]. The digitization of assets makes the value of assets have the characteristics of verifiability, transferability and detachability, which greatly improves the liquidity of digital assets. All transactions on the chain are jointly participated by multiple parties, and all parties have complete transaction data to ensure the authenticity of information such as contracts, orders, and payments. The energy Internet strategy has led to a sharp increase in emerging businesses, and issues such as data integration, equipment security, and multi-agent coordination have gradually become prominent, restricting the coordinated development of the upstream and downstream of the industry chain. BcT solves the problem of the authenticity of the identity of the participants. The security model based on cryptography ensures that the transaction cannot be denied, and has strict authentication requirements for the identity authentication of each link of the transaction.

In response to the application requirements of power business synergy, this article relies on the characteristics of multi-point maintenance and data coordination, using smart contracts, consensus mechanisms to build an open, transparent and fair power supply financial chain, to realize the transition from weak business connection to strong data interoperability, promote the construction of a new business sharing ecosystem, and enhance the credible sharing of business data in the power industry. The core enterprises rely on the power supply financial chain to provide comprehensive financial services for upstream and downstream enterprises, to improve quality and efficiency of corporate operations, and to collaborate with financial capital and real economy to build an industrial ecosystem of mutually beneficial coexistence and sustainable development of financial institutions, enterprises and supply chains [14,15]. Figure 4 shows blockchain public services for the power industry, carrying shared services such as deposit certificates, transactions, and coordination, building a fair and credible ecosystem for customers, and promoting distributed transaction settlement, and judicial deposits. Businesses such as certification and network security are carried out. At present, the blockchain-based power supply chain finance has realized "order financing" and "accounts receivable factoring" financing loans exceeding 30 million yuan, and under the premise of close to zero cost, it provides legal effect for millions of photovoltaic users online contracting service. Meanwhile, information such as enterprise industrial and commercial data, electricity bill payment data,
supplier evaluation information are recorded on the chain to provide strong support for multi-
dimensional enterprise credit evaluation.

With the deepening application of blockchain in the field of power commerce, power companies
have actively carried out exploration research in the fields of electricity bill finance, photovoltaic
cloud network, big data credit investigation, electronic invoices, and judicial deposits. At present, the
total amount of data on the chain exceeds 4.3 million, and 26,000 data on the transaction order of
electricity bill financial products "e-e-loan" have been deposited on the chain, serving more than
10,000 small, medium and micro enterprises, and the credit amount reached 1.618 billion yuan. At the
same time, companies actively carry out the in-depth integration of BcT, financial management, order
information and other data to the chain for evidence, to achieve efficient sharing, secure transmission,
and multi-agent coordination of electronic invoices, avoiding false bills and the financial risks brought
by repeated reimbursements have improved the company’s ability to control financial risks.

The supply chain of electric power enterprises is constantly changing and extending, the difficulty
of management is further increasing, and the efficiency of coordination is facing many constraints,
which are mainly manifested in data island, data trust and performance guarantee. There are multi-
level supply and sales relationships in the supply chain, but the credit of core enterprises can only
cover the first-class suppliers and first-class dealers who have direct trade relations with them, and
cannot be transferred to the upstream and downstream SMEs who need more financial services. As
shown in Figure 3, building the supply chain based on the BcT can open up the transaction
relationship between the main bodies, realize the transmission of credit between the core enterprises
and the remote enterprises, and expand the scope of financial services based on the supply chain.

6. Conclusions
In view of the risks in the power IoT environment, this paper proposes the use of BcT to enhance the
security of data interaction, so as to achieve high-level protection of data circulation in all links of the
power network. Power terminals are characterized by huge numbers, large-scale systems, and limited
computing power. The innovation of ICT has introduced new security risks to the construction of
power networks. The power terminal has a wide deployment range, uncontrolled on-site environment,
and complex vulnerability risk handling. Attackers can use the terminal’s software, hardware, and
system defects to carry out diversified attacks, posing a huge threat to energy network.

Acknowledgment
This work was supported by the Science and Technology Project of State Grid Corporation of China
(No. 5700-201916465A-0-0-00).

References
[1] Peng D, Wei T, Yao J, et al, 2019 Information security protection of distributed energy
stations under the environment of energy internet vol 52 no 10 (Electric Power) pp 11-17, 25.
[2] Zhang T, Zhao D, Xue F, et al, 2019 Research framework of cyber-security protection
technologies for smart terminals in power system vol 43 no 19 (Automation of Electric Power
Systems) pp 1-8, 67.
[3] Wang D, Shi X, Chen Z, et al, 2018 Research on the smart contract of block chain
technology in supply chain vol 9 no 8 (Cyberspace Security) pp 8-17.
[4] Zhao Y, Peng K, Xu B, et al, 2019 Status and prospect of pilot project of energy blockchain
vol 43 no 7 (Automation of Electric Power Systems) pp 14-22.
[5] Han D, Zhang C, Sun W, et al, 2019 Framework design of smart distribution trading
platform based on blockchain technology vol 43 no 7 (Automation of Electric Power Systems)
pp 89-96.
[6] Zeng S, Huo R, Huang T, et al, 2020 Survey of blockchain: principle, progress and
application vol 41 no 1 (Journal on Communications) pp 134-151.
[7] Chen Z, Peng T, Zhang Y, et al, 2020 Distributed network data security protection for SG-eIoT vol 1075 (Advances in Natural Computation, Fuzzy Systems and Knowledge Discovery) pp 935-943.

[8] Shi J, Li R, 2019 Survey of Blockchain access control in internet of things vol 30 no 6 (Journal of Software) pp 1632-1648.

[9] Zeng J, Liu Y, 2020 Trust management of blockchain terminals in energy consumption monitoring vol 40 no 8 (Electric Power Automation Equipment) pp 31-37.

[10] Chen X, Zhu Y, Feng K, et al, 2020 Identity authentication of power system safety and stability control terminals based on blockchain vol 38 no 2 (Journal of Guangxi Normal University (Natural Science Edition) pp 8-18.

[11] Han D, Zhang C, Sun W, et al, 2019 Framework design of smart distribution trading platform based on blockchain technology vol 43 no 7 (Automation of Electric Power Systems) pp 89-96.

[12] Cai Y, Gu Y, Luo G, et al, 2020 Blockchain based trading platform of green power certificate: concept and practice vol 44 no 5 (Automation of Electric Power Systems) pp 1-9.

[13] Xie K, Zhang X, Zhang S, et al, 2020 Application and prospect of blockchain technology in electricity trading vol 44 no 19 (Automation of Electric Power Systems) pp 19-28.

[14] Hou W, Wu H, Gao F, et al, 2020 Research on profit allocation of power supply chain based on block chain smart contract vol 33 no 1 (Journal of Xinyang Normal University(Natural Science Edition) pp 144-148.

[15] Wang L, Yang Q, Wang J, 2020 Application analysis of photovoltaic micro-grid transaction marketization based on the block chain vol 57 no 12 (Electrical Measurement & Instrumentation) pp 75-82.