Analysis of the Application Status and Trend of Blockchain in Data Management

Guang Chen[1,a *], Weiping Cui[1,b], Yong Yan[2,c] and Yixin Sun[1,d]

[1]State Grid Energy Research Institute Co. Ltd., Beijing 102209, China

[2]State Grid Zhejiang Electric Power Co., Ltd. Research Institute, Hangzhou 310027, China

[a]chenguang@sgeri.sgcc.com.cn, [b]cuiweiping@sgeri.sgcc.com.cn, [c]yanyong@zj.sgcc.com.cn, [d]sunyixin@sgeri.sgcc.com.cn

[*]corresponding author

Keywords: Blockchain; Data Management; Application Field

Abstract: Because some characteristics of blockchain itself are very in line with the needs of certain specific businesses, so far, blockchain technology has been widely used in many fields, which mainly include: pan-finance, industrial supply chain, network file storage, credit management and some other fields. This paper comprehensively analyzes the application status and development trend of blockchain in data management, in order to provide reference for relevant researchers.

Data management platform based on blockchain technology can solve many problems.

First, the data and transfer transaction records on the blockchain-based power data management platform cannot be tampered with. Although we rarely hear in the real world that the content of the electricity data itself is tampered with, the possibility of this cannot be avoided. And more importantly, when the management platform involves access to multiple shared or trading data or data, these records can be tampered with, falsified and leaked as long as people involve human operations. Obviously, no matter which situation is the security problem of the data management platform, which will cause great harm to the power data management. The characteristics of blockchain cannot be tampered with, unrevoked, and recorded in every action, making the correctness and uniqueness of the power data guaranteed.

Secondly, the security guarantee brought by high redundancy. Each node has a backup in the blockchain, which makes a single point of failure not compromising data integrity. It is well understood that if the entity puts its own power data or access on the data management platform built through blockchain technology, then the entity has power data or access will exist in the form of decentralized or multicenter node backup, which ensures that the power data and shared transactions cannot be lost, because the failure of a single independent node does not lead to the overall failure of the blockchain. The private key in the hands of the entity ensures that only the private key holder in the blockchain as a whole is eligible to view the security of the power data.

Blockchain technology can achieve the complex permission custody of multi-private keys. At present, the storage of many sensitive data in the Internet society, many data can be easily transferred and used on the Internet, which is not a good state, and the blockchain multi-private key authority storage mode can well prevent this kind of situation. With a smart contract, you can set up multiple private keys to assign individual information data, and have a rule to make each access to the data, and several private keys must be authorized simultaneously. Blockchain this technology ensures the normalization and legalization of sensitive power data in network use.

Based on the characteristics of the blockchain system, the use of the blockchain system can bring new data management modes to a large number of domain application systems. At present, each application field has formed an initial accumulation in the blockchain technology, gradually combining the functions of the blockchain system with the original business system, making the use of the blockchain characteristics to solve the disadvantages of the business system, and improving the shortcomings and limitations of the blockchain system itself. Now, applications in various areas

have posed more new challenges to blockchain systems.

1. Pan-financial Applications

In the field of pan-financial application, the blockchain system can provide safer and more convenient automatic transaction and accounting services for financial payment and management scenarios such as cross-border payment, supply chain finance and digital bills. In cross-border payment applications, many enterprises have started to make relevant attempts. The early work mainly focused on using virtual currency to provide low-cost cross-border remittances for small and medium-sized enterprises, while the current financial institutions such as banks are committed to further improving the efficiency of cross-border payment with the high throughput of the alliance chain and the efficiency of high-recognition characteristics. Compared with the 10% rate of the early VISA system and the arrival time of one week, Ant Financial related systems based on blockchain structure have been able to achieve 1 minute of arrival, with an average efficiency of 1 0,000 times, but also has a lower payment cost. For bills and supply chain financial business, financial institutions can use blockchain technology to realize distributed management of bill assets, store assets data in blockchain, so that relevant personnel of assets can realize point-to-point value transmission, without the control and verification of physical bills and centralized system. The blockchain-based supply chain mechanism reduces the cost of intermediate labor participation, and realizes end-to-end transparency, thus improving the efficiency of asset information processing while reducing the management costs.

In the financial field, distributed storage, information sharing and imtamper fiable characteristics of applied blockchain system are managed data, and transaction records, payment records and digital assets and other data are distributed stored in participating nodes in the way of full sub-copy. The financial sector mainly uses the alliance chain system to ensure security through the participant access mechanism and a simpler consensus mechanism to ensure the system efficiency. However, blockchain systems still need to address the limitations of transaction processing efficiency, cross-chain interaction, and automated processing of complex behaviors to better support financial services.

First, the blockchain system also needs to be further improved in the real-time performance and throughput of the transaction verification. The existing VISA system can support thousands of transactions per second, and the Alipay system has reached a peak of 85,900 transactions per second, while the EOS system using the DPoS consensus mechanism is 3,000 per second, and the DAG structure-based IOTA system is 3,000 per second. Visible blockchain system processing capacity is not enough to replace the existing centralized trading system. Therefore, the blockchain system also needs to continuously improve the consensus mechanism to adapt to the high-throughput financial trading applications.

Secondly, the future blockchain system needs to support the cross-chain data interaction function. There are several financial organizations in the existing financial field, which also means that there will be multiple blockchain systems in the future financial field, and each block chain system stores a heterogeneous data structure. Payment transactions between different financial organizations need to be realized through cross-chain interaction, so as to solve the problem of different heterogeneous data access in blockchains.

2. Industrial Supply Chain Field

There are often hundreds of processing links in industrial supply chain systems, and such a large number of nodes bring great challenges to the tracking and management of the supply chain. In the supply chain, commodity-related aspects of production, transportation and sales need to record a lot of process information. Using the blockchain system to store and manage the supply chain system data can effectively provide core functions such as deep traceability, inquiry and verification of the supply chain process information, thus improving the transparency and security of the industry. Take the beverage supply chain as an example, under the original mechanism, the manufacturer

cannot obtain subsequent sales information after the agent takes the goods. Through the blockchain system, we can easily integrate production data and sales data, on the one hand, it is convenient for final consumers to trace the goods, and on the other hand to provide transparent data management for manufacturers. In practical application, blockchain also needs to further improve information security, build a traceability mechanism and establish dislocation incentive measures to support the application of the industrial supply chain.

In terms of security, due to the transparency of information sharing in blockchain systems, the risk of privacy information. The existing mechanism is mainly to use digital signature and public-private key encryption and decryption mechanism to ensure information security, which requires the blockchain system to achieve a more efficient intelligent contract mechanism, on the one hand, to simplify the supply chain process to improve business processing efficiency, on the other hand to provide automatic signature verification to prevent privacy data disclosure such as personal information.

In terms of data traceability, the blockchain system also needs to further build a traceability model more consistent with the industrial supply chain process, so as to find out cheating in each link of the supply chain process in a timely and efficient manner. The combination of traceability mechanism and intelligent contract will be able to realize the automatic management system based on technology and algorithm.

In terms of incentive mechanism, blockchain needs to implement dislocation incentives. The supply chain system should design reasonable incentives for all participants to effectively ensure that participants join the blockchain system and ensure the quality of data input into the blockchain.

3. Network File Storage Domain

In the field of network file storage, the blockchain system can build a public chain storage platform, provide personal data storage and sharing services, and realize the sharing mechanism, traceability mechanism and right confirmation mechanism of data resources. There are currently some public chain systems for file storage, such as IPFS and Sia. The primary goal of these systems is to build a decentralized distributed data storage that reduces the bandwidth and storage costs of network files. Through the combination of public blockchain systems and distributed data storage platforms, you can build file storage ecosystems including file data storage, sharing, governance, and value-added value. The existing blockchain distributed storage mechanism is decentralized and solves security and throughput problems, but there are still deficiencies in programmability, scalability and confirmability, which is also the main challenge facing blockchain-based network file storage.

Programmatability mainly refers to the writing of the execution process of file data transaction into the programmable language of smart contract, and ensures the automaton and integrity of transaction execution through the code mandatory operation mechanism of smart contract. The current smart contracts mainly support the automatic execution of transfer transactions, while they are less proposed for smart contracts and programmable languages that support data governance.

Scalability refers to that with the expansion of the number of nodes in the system, the number of files increases, the system will not decrease significantly. Since the network file storage is mainly running in the form of a public chain, the corresponding blockchain system will not use the efficient consensus algorithm after the node reaches a certain scale, and this problem will result in a decrease in throughput and scalability.

Confirmation ability mainly refers to the documents in the network can confirm the original owner of the document based on the blockchain traceability mechanism after replication, so as to avoid copyright disputes in the file storage system. True file management requires blockchain to combine traceability mechanism with metmeta-information management mechanism of distributed storage, which poses another new challenge to network file storage.

4. Credit Investigation Field

In the field of credit investigation management, the original centralized system needs to gather, sort out and release the shared credit data of the participating institutions, and there is still the problem of the credibility of third-party deposit certificates. Based on blockchain management credit information, participating institutions can build an alliance chain structure and share their credit data. At this time, the blockchain system has its own information that cannot tamper with, data encryption authorization protection, intelligent contract and other characteristics can effectively solve the problem of credit information island in the original credit investigation system, improve the system security and reduce the operating cost of credit investigation. However, due to the closure of the existing system in the traditional credit investigation field, there is still a great risk to use blockchain system replacement, and blockchain also faces many technical challenges in credit investigation management, including the following aspects:

First, the privacy protection of data. Blockchain-based credit platform makes all nodes participate in data maintenance through the mechanism, which makes 51% malicious attack difficult to ensure the system has the security of data tampering, but because the chain data all disclosed, even if the encryption method using the public key private key still has the risk of private data leakage, so the system needs to support the control mechanism of the chain data, to avoid data sharing parties.

Secondly, the data quality control on the blockchain. The credit investigation data provided by multi-participants has potential data quality problems such as inconsistent data and redundant data. How to realize eliminating redundant data and ensuring data consistency in the tamper-proof blockchain credit investigation system is another challenging problem in the research of blockchain distributed data management.

Again, the on-chain management of diversity data. Credit investigation data has multimodal characteristics, covering structured records, document files, fair certificates, and even voice and mail data types. To do end, the blockchain system needs to provide the function of chain storage on multiple data types and is capable of automated verification processing based on these files.

5. Other Application Areas

In addition to the above several major application areas, blockchain can also be applied to all kinds of areas with distributed data storage and related requirements:

(1) Distributed social networking

Distributed social networks are constructed based on P2P technology, using a decentralized structure, while all the data are scattered among the network nodes. Constructing a distributed social network based on a blockchain system can avoid a single-point failure through decentralized social interaction, realize diversified incentive mechanisms, have a good privacy protection mechanism, and reduce operating costs through an incentive mechanism, such as the Steem system. However, distributed social networks need to operate using public chain modes, and large-scale social network blockchain systems will face serious consensus efficiency and decentralized balance problems. Taking the Steem system as an example, the current use of the DPoS consensus mechanism reaches a consensus through 21 witnesses to ensure the system throughput rate, but there is a potential risk of centralization.

(2) Charity field

Blockchain system has a trust mechanism built as a new trust mechanism based on distributed storage and consensus algorithms, which can realize transparent, open and effective supervision of public welfare information and help in the field of public welfare solve trust problems. Blockchain system can record all the information such as donation projects, raising details, fund use and beneficiary feedback in the public welfare process. At the same time, a number of public welfare organizations, payment institutions and audit institutions constitute a multi-party alliance chain to improve the security of the system information. Its application challenges mainly come from the mismatch between complex public welfare scenarios and simple transaction bookkeeping methods,

which needs to be solved by building intelligent contracts that comply with the complex public welfare process.

(3) Education and employment field

In the field of education and employment, students ' student status information, academic status information, and inauguration information should be managed. There are a large number of information islands in the original scattered information management system of information, employment. Each educational institution only manages the information of students involved in themselves, thus leads to the face of academic fraud, school status fraud, resume fraud and other problems in the process of employment and enrollment, and the lack of effective verification mechanism in units and universities. The data transparency and tamper-free characteristics of the blockchain system can effectively build a credible educational certification mechanism, and supports the controlled access and automatic verification of student educational employment information by the encrypted storage of student educational proof information on the blockchain. Because educational data can also be regarded as a kind of credit investigation data, blockchain faces similar challenges to the field of credit investigation management in the field of education and employment.

Acknowledgments

This work is supported by the science and technology project of State Grid Corporation of China (Research on Key Technologies of capitalized operation and value mining for power data, grant no.5100-201957475A-0-0-00)

References

[1] Swan M. Blockchain: Blueprint for a New Economy [M]. Sebastopol: O'Reilly Media, 2015.

[2] Nakamoto S. Bitcoin:A peer-to-peer electronic cash system [DB/OL]. (2008-10-31). https://bitcoin.org/bitcoin.pdf.

[3] Dantheman. DPOS Consensus Algorithm-The Missing White Paper [DB/OL]. (2017-05-29). https://steemit.com/dpos/@dantheman/dpos-consensus-algorithm-this-missing-white-paper.

[4] Castro M, Liskov B. Practical Byzantine Fault Tolerance [C] // New Orleans: USENIX OSDIO, 1999.

[5] Nick Szabo. Smart Contracts: Building Blocks for Digital Markets [J]. Entropy: The Journal of Trahumanist Thought, 1996(16).

[6] Xiong Li Bing, et al. Proficient in Ethereum Smart Contract Development [M]. Beijing: Electronic Industry Publishing House, 2018

[7] Chamber of Commerce (CDC), Smart Contract Alliance (SCA). Smart Contracts: 12 business and other use cases. 2017.