Research on Terminal Communication Security Access System Technology Based on Blockchain

Wu Lijie[1,a,*], Liu Yan, Dong Kaili, An Zhiyuan

[1]State Grid Henan Information & Telecommunication Company, Zhengzhou, 450000, China

Keywords: Blockchain, Authentication System

Abstract: As an important part of power communication network and the extension of backbone communication network, terminal communication access network is responsible for collecting information of terminal service application access point and sending various control interactive instructions. At present, the access network is still constructed according to the needs of different majors, emphasizing the self-use of each service, and no public communication transmission channel has been formed. There is a lack of research on the adaptability, security partition and performance requirements of the carrying services of the access network for multi-service access. Aiming at the problems existing in terminal communication access network, This paper studies the research of terminal communication security access architecture based on blockchain, designs a decentralized authentication system, and realizes the decentralized secure access mechanism of terminals, networks and services.

1. Introduction

As a decentralized peer-to-peer trusted network of distributed storage, blockchain [1] is the core supporting technology of the digital crypto currency system represented by bitcoin. Blockchain technology is highly transparent, decentralized, untrustworthy, collective maintenance (unchangeable), anonymous and so on, able to realize point-to-point transaction, coordination and collaboration based on decentralized credit in a distributed system where nodes do not need to trust each other by means of data encryption, timestamp, distributed consensus and economic incentive, providing a solution to the problems of high cost, low efficiency and insecure data storage in centralized organization. Based on the blockchain technology, this project can significantly improve the level of security and credibility of the network environment for data sharing through the research of scenario and technology adaptation analysis technology and the research and development of the prototype system, so as to meet the growing demand for security and credibility.

2. The Security of Terminal Communication Access Network

The terminal communication access network is an extension of the backbone communication network[2], which takes the terminal boundary and terminal equipment of the backbone communication network as the demarcation point to realize the effective data transmission between the business main station and the terminal equipment. However, the access network has the characteristics of multiple carrying services, scattered distribution, and harsh environment, making it impossible to adopt a single technology to realize networking. The core problem of secure and trusted access for ubiquitous service of power communication is how to use customized and unified communication terminal to support its secure and trusted access[3].How to guarantee the secure and trusted access of ubiquitous service has become an important problem in the secure and trusted access of power communication network.

The existing power communication network ubiquitous service access solutions are mostly completed by the centralized management and control institutions of power grid companies. With the increasingly large ubiquitous business system of power communication network, the task of centralized management organization is intensified, resulting in low credibility of basic data and poor process timeliness [4]. In contrast, decentralization is more efficient. For example, if the

DOI: 10.25236/icbsis.2020.039

surplus electricity of a home photovoltaic power station is provided to a neighbor's appliance, the transaction can be completed directly on the basis of mutual trust, achieving higher efficiency. Blockchain enables untrusted, point-to-point communications that can be Shared across billions of devices on the same network without the need for traditional expensive resources, whose technical characteristics are consistent with the concept of power communication ubiquitous service, which makes it potential to become one of the important technical solutions for power communication ubiquitous service secure and trusted access in the future. However, it is necessary to further clarify the application mode of blockchain in the field of secure and trusted access of power communication business and give corresponding reasonable solutions. How to apply block chain technology, combining with the safe and reliable access data access, transmission, processing and application requirements of the power communication business and the characteristics of each part, to establish a unified power communication business security trust access architecture is the foundation and key of the research.

3. Blockchain Technology

Blockchain technology provides a standard for resolving conflicts of authority between different suppliers, giving everyone equal rights, and facilitating collaboration between transaction processing and interactive devices[5].Distributed ledger based on blockchain can provide trust, ownership record, transparency and communication support for power communication network, and store transaction information in a private chain. The architecture that uses centralized servers to collect and store data allows information to be written to local ledgers and synchronized with other localized ledgers, ensuring the security and uniqueness of the facts. All device operations on the blockchain are timestamped to ensure traceability. The real innovation in blockchain is digital protocols, or smart contracts, that can be applied to blockchain data and perform standardized processes in the operation of devices. And blockchain with high-end encryption technology can solve the problem of illegal device intrusion.

Generally speaking, blockchain system is composed of data layer, network layer, consensus layer, incentive layer, contract layer and application layer [6]. The data layer encapsulates the underlying data block and related data encryption and time stamping techniques. The network layer includes distributed networking mechanisms, data dissemination mechanisms, and data verification mechanisms. The consensus layer mainly encapsulates various consensus algorithms of network nodes. The incentive layer integrates economic factors into the block chain technology system, mainly including the issuance mechanism and distribution mechanism of economic incentives. Contract layer is used to encapsulate various scripts, algorithms, and intelligent contracts, which is the basis of the programmable feature of block chain. The application layer encapsulates various application scenarios and cases of blockchain. In this model, time-stamp-based chain block structure, distributed node consensus mechanism, consensus-based economic incentives, and flexible programmable smart contracts are the most representative innovations of blockchain technology. Combined with the business characteristics of the power industry, the technical architecture of the design blockchain is as follows.

Data layer: The narrow blockchain is the data book shared by each node of the decentralized system. Each distributed node can use a specific hash algorithm and a Merkle tree data structure, and the transaction data and code received over a period of time are encapsulated into a time-stamped data block, linked to the current longest main block. On the chain, the latest blocks are formed. The process involves technical elements such as blocks, chain structures, hashing algorithms, Merkle trees, and timestamps.

Network layer: The network layer encapsulates the networking mode, message propagation protocol, and data verification mechanism of the blockchain system. According to the actual application requirements, the specific propagation protocol and data verification mechanism are designed, so that each node in the blockchain system can participate in the checksum accounting process of the block data. When the block data is verified through most nodes in the network, it can be recorded in the block chain.

Consensus layer: the blockchain consensus layer encapsulates these mechanisms that enable each node to reach an efficient consensus on the validity of block data in a decentralized system with highly decentralized decision rights.

Incentive layer: The consensus node in the decentralized system itself is self-interested, and the maximization of its own revenue is the fundamental goal of its participation in data verification and accounting. Therefore, it is necessary to design a reasonable crowdsourcing mechanism with incentive compatibility, so that the individual rational behavior of the consensus node to maximize its own benefits is consistent with the overall goal of ensuring the safety and effectiveness of the decentralized blockchain system. The blockchain system integrates large-scale nodes and forms a stable consensus on the history of blockchains by designing moderate economic incentives and integrating them with the consensus process.

Contracts layer: layer encapsulates the various types of script code, algorithm of block chain system and the resulting more complex intelligent contract. If the data, network and consensus on three levels, respectively, as the underlying block chain \ virtual machine for data representation, data transmission and data validation function, contract layer is based on virtual machine block chain business logic and algorithm, is to realize the flexible programming and operating data block chain system.

Application layer: application layer encapsulates various application scenarios and cases of blockchain. Under the scenario of trusted power communication network, it is embodied in power system, power finance, enterprise management, power security, etc.

Blockchain technology has been preliminarily verified on the Internet of things. American blockchain technology company Filament is committed to using blockchain technology to upgrade the Internet of things system, to realize the control of each key link, and reduce unnecessary resource consumption and cost. Filament has built an open technology stack that leverages today's most advanced communication and security methods to enable devices to discover, communicate, and interact with each other in a fully autonomous and distributed manner. Take the deployment of the railway network, in which locomotives, freight and passenger cars, on-off motors and other infrastructure are connected via cheap surface-mounted devices such as Filament taps and can communicate with each other via radio (such as tap) rather than relying entirely on Wi-Fi, cellular or satellite access. Now the rail network can collect real-time data from all these devices in a variety of network conditions, and the devices can respond in real time and upload data to run preventive analysis, enabling more targeted maintenance and reducing the risk of hazards and the cost of accidents. In addition, the equipment involved can directly or indirectly exchange the value of the entity. For example, they could sell data on environmental conditions to the weather service, data on the use of the rail network to businesses specialising in statistics. As these examples show, the exchange of value is not limited to a single value location or vertical direction and can be achieved across organizations in a secure and flexible way.

4. Terminal Communications Security Access System Based on Blockchain

The research framework of the secure trusted access application scenario to be adopted in this time is shown in Figure 1. In the stage of data perception and access, the ubiquitous service data of power communication is collected by a large number of service terminals and communication terminal devices such as concentrator and collector[7], and the data privacy control and data sharing capability are realized through the data sharing platform deployed on the data transmission channel. In order to realize this function, the data sharing platform is designed through the unforgeable, non-tamper able, traceable, trusted authentication features and decentralized access capabilities of the blockchain technology, and the data sharing isolation capability provided by the digital asset identification service. The power communication is ubiquitous in the service data security trusted access architecture to ensure the secure and trusted access and shared storage of the service data. At the same time, different service systems can access the required ubiquitous traffic data of the power communication according to the data identification and realize the efficient application of the ubiquitous service data of the power communication.

The terminal and data access link include the new terminal equipment with both the business capability and the secure and trusted communication capability and the communication terminal equipment with the secure and trusted communication capability[8].The new type of terminal equipment realizes data sharing with all kinds of business systems through the distributed data trusted chain, and the communication terminal equipment with the ability of secure and trusted communication interconnects with the interface of the existing metering terminal equipment to realize secure and trusted access. In the service link of blockchain, the existing mature public chain platform can be directly used to realize the trusted storage and sharing of all kinds of transaction data, or the trusted chain can be built separately to realize the sharing of all kinds of transaction data. Since the service cost of public chain application is not controllable, this paper intends to choose the latter approach, which requires the comprehensive consideration of different roles such as business, supervision and technical support, and the establishment of no less than 4 (the minimum 3) trusted chain nodes, and the establishment of maintenance mode of relevant nodes to ensure the reliable operation of blockchain services. In the link of business application, after the introduction of block chain technology, on the basis of ensuring data security, trust and sharp-sharing, the corresponding data gateway is set for the existing system to realize data access to the old system. For the new system based on block chain technology, data access can be directly. Research on key technologies is carried out from the three links of blockchain service, terminal and data access, and business application, so as to solve the mechanism of equipment and data access authentication, security and trusted sharing service in blockchain link.

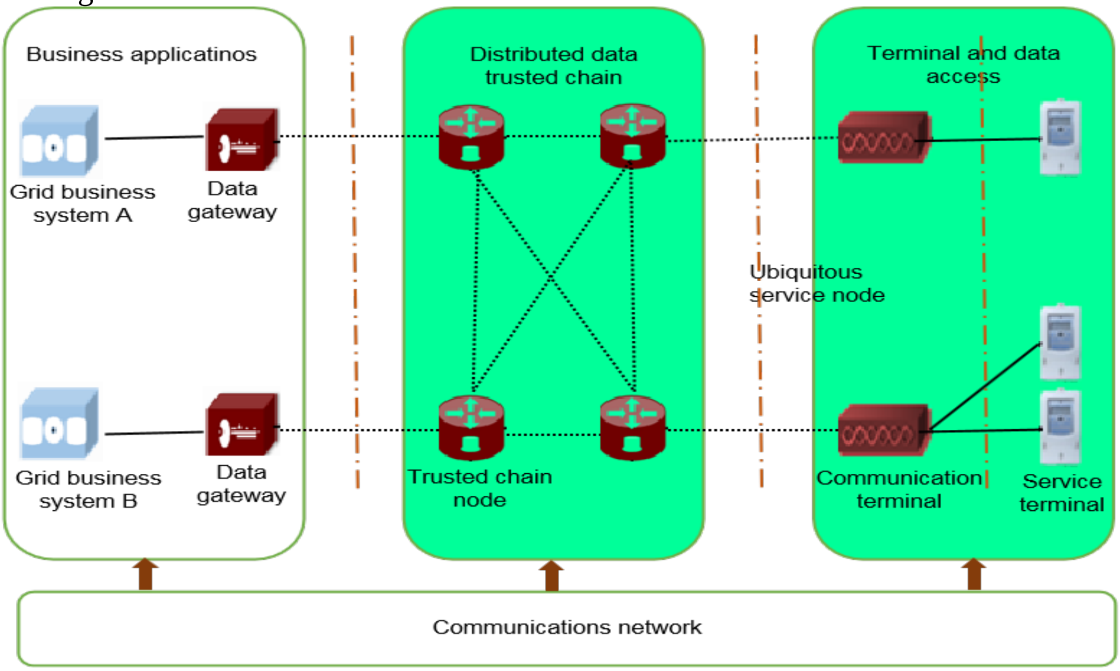

Fig.1. The ubiquitous service access application scenario carried by a terminal communication access network based on the blockchain

5. Conclusion

In view of the security, trust and flexibility of the ubiquitous service of terminal communication access network, combined with the business security reliable communication terminal access generic access of data access, transmission, processing and application requirements of each part and characteristic analysis, this paper standardizes the ubiquitous secure and trusted access mode and access terminal of terminal communication access network, defines the data processing, storage and sharing mechanism, and gives the business application mode of the ubiquitous secure and trusted access platform of terminal communication access network. It proposes a secure and trusted access architecture for ubiquitous service of power communication based on block chain technology to support secure and trusted access of ubiquitous service of terminal communication access network.

References

[1] Marijn Janssen,Vishanth Weerakkody,Elvira Ismagilova,Uthayasankar Sivarajah,Zahir Irani. A framework for analysing blockchain technology adoption: Integrating institutional, market and technical factors[J]. International Journal of Information Management,2020,50.

[2] Mukherjee,B. WDM optical communication networks:progress and challenges [J].IEEE Journal on Selected　Areas in communications.2000.18(10):1810-1824.

[3] Skorin-Kapov,N.,Furdek.M.,Zsigmond. S.et al.Physical-layer security in evolving optical networks[J].IEEE Communication Magazine,2016,54(8）：110-117.

[4] Lazzez,A. Notice of Violation of IEEE Publication Principles All-optical networks: Security issues analysis[J]. IEEE/OSA Journal of Optical Communications and Networking,2015,7(3):136-145.R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[5]Shrier,D., Wu. W., Pentland A. Blockchain & infrastucture(identity,data security)[J].Massachusetts Institute of Technology-Connection Science.201,1(3).

[6] Chen.W.,Jacidi,B., Chen,X. Advances in optical security systems [J].Advances in Optics and Photonics.2014,6(2):120.

[7]Yang,H., Zheng, H., Zhang,J.,et al. Blockchain-based trusted authentication in cloud radio over fiber network for 5G [A]. //2017 16th International Conference on Optical Communications and Networks(ICOCN)[C]. Wuzhen.China:IEEE,2017:1-3.

[8]Yang,H., Zheng, H., Zhang,J.,et al. Blockchain-based trusted authentication in cloud radio over fiber network for 5G [A]. //2017 16th International Conference on Optical Communications and Networks(ICOCN)[C]. Wuzhen.China:IEEE,2017:1-3.