Application of wireless sensor network based on blockchain architecture technology in action capture

Jingyang Cao[1], Shirong Yin[1], Tianhong Luo[2*]

[1]School of Mechanotronics & Vehicle Engineering, Chongqing Jiaotong University, Chongqing 400000, China

[2]School of Mechanical--Electrical Engineering, Chongqing University of Arts and Sciences, Chongqing 402160, China

Keywords: blockchain, wireless sensor network, cloud computing

Abstract: in recent years, with the continuous development of mobile Internet, intelligent terminal and cloud computing, the application of various sensor terminals (such as intelligent wearable devices, smart cars, smart home) tends to mature. All kinds of sensor terminals have the characteristics of mobility and miniaturization, and their communication channels are more dependent on wireless network, and the data transmission mode is more flexible. At the same time, wireless sensor terminals also face various security problems. This paper will focus on the wireless terminal security technology based on the blockchain technology, and propose a wireless terminal security architecture based on the blockchain technology system, and research from the data layer blockchain data structure definition, network layer distributed networking design, consensus layer efficient consensus algorithm design, application layer monitoring and auditing and other aspects. This paper studies the real-time follow-up of blockchain technology development, laying a technical foundation for wireless terminal security system, and providing new ideas for wireless terminal security research.

1. Feasibility of wireless terminal security guaranteed by blockchain Technology

All kinds of wireless sensor terminals are mainly used for information acquisition, acquisition and object recognition. Sensors, cameras, identification codes and real-time positioning chips are used to collect all kinds of identification, physical quantities, audio and video data, and then the preliminary data processing is realized through short-distance transmission, ad hoc network and other technologies. The mobile characteristics of wireless sensor terminals break the traditional network boundaries, and vulnerable wireless terminal nodes are more likely to become the target of attack. There are more and more attacks against wireless sensor terminals, including physical attacks, forgery or counterfeiting attacks, signal leakage and interference, resource depletion attacks, privacy leakage threats, etc. The security problem of each wireless sensing terminal will be magnified exponentially in wireless network, and the final security risk loss caused by a single terminal node is immeasurable. Therefore, for the massive and diversified wireless sensing terminals, it is necessary to be able to monitor and respond to the security threats of each terminal node in real time, so as to improve the security protection and anti attack ability of each terminal node.

2. Analysis on the technical characteristics of blockchain

Blockchain is a decentralized distributed database, which combines data blocks into a chained data structure according to the time sequence, and uses cryptography to ensure that the information can not be tampered with or forged. Blockchain technology combines P2P and asymmetric encryption technology, and is suitable for distributed systems. It has the characteristics of decentralization, traceability, tamper resistance, autonomous peer-to-peer, and contract execution.

  DOI: 10.25236/isaiee.2020.005

2.1 Chain storage structure

The blockchain connects the blocks in chronological order and distributes in the whole network to form a network wide consensus information storage system. The chain storage structure is shown in Figure 1. The nodes in the blockchain are based on the latest blocks generated on a known and recognized "chain". Each block is identified by its password hash, and each block refers to the hash value of the data block generated in front of it, forming a chain of data blocks. Each data block in the blockchain contains a column of transactions and a hash value of the previous block to ensure that the data can not be tampered with. Any node in the network can access this ordered, backward linked list of data blocks to read network data.

In the distributed system, the nodes in the blockchain network must be synchronized. Since each block can only be followed by the latest block, and the next block can only be generated after the latest block, so as long as the synchronization message is received, it must be synchronized immediately. Only through massive calculation can the effective hash of the current block be obtained, and only the hash meeting the conditions can be accepted by the blockchain, which is called "mining".

2.2 Distributed Autonomy

Distributed autonomy means that all nodes in the distributed network cooperate with each other to maintain the consistency of distributed data, including the automatic generation and verification of new nodes, and the consensus reached through negotiation among nodes, so as to prevent the execution of malicious and unauthorized operations without the participation of trusted third parties.

Based on the analysis of the block chain data structure, how to ensure the synchronization of all nodes in a distributed system is the realization of consensus, which is the core of the normal work of the distributed system. However, due to the introduction of many nodes in the distributed system, node failure, fault or downtime will directly affect the normal operation of the distributed system. There is no way to achieve strong consistency and availability in a distributed system because of the delay of the network. A system with strong consistency that leads to a decrease in system availability, and that accepts requests and hands them off to other nodes, does not solve the problem for highly concurrent services. Therefore, final consistency is selected in the current mainstream distributed systems. The final consistency allows the state conflict of multiple nodes, but all the nodes to communicate can resolve the conflict within a limited time, and the inconsistent state can be restored to be consistent, so as to ensure that the nodes can directly communicate normally.

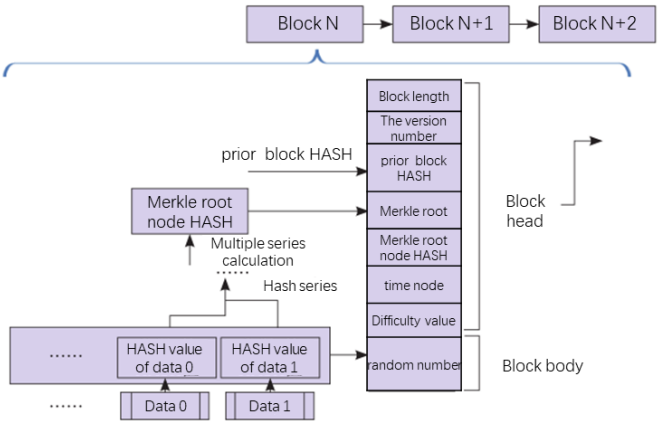

Fig. 1 Block Chain Structure

Therefore, the main problem of block chain consensus is how to design a consensus mechanism, which can make the transaction data verified by more than half of the nodes in the set of the consensus participating nodes without trusting them, and store the data distributed in each data storage node in a specific structure. Current consensus algorithms applicable to block chain include Byzantine fault tolerance mechanism (BFT), proof of Workload (POW), and proof of interest (POS) [5].

Byzantine fault tolerance (BFT), which builds trust in trustless network nodes, prevents malfunctions or malicious nodes from causing misbehavior that affects the formation of final consistency. The algorithm is limited by network size. POS requires a node that commits a generated block to adopt the new hashing algorithm and provide POW it performs. The proof of the system requires at least half of the network hash or computing power. POS is another consensus algorithm used in block chain networks. Based on the interest in the password in the currency, the next block is selected randomly according to the shares and timing of different nodes. Rewards and punishment mechanism is introduced to reduce the workload [6], but when dealing with BFT, the impact of malicious nodes cannot be minimized.

According to the distributed features of wireless network and practical application, it is an urgent problem to select the appropriate consensus algorithm and improve the existing consensus algorithm to meet the low computing capacity and low storage of wireless terminals.

2.3 Intelligent Contract

Intelligent contract is a protocol program in block chains. The interaction between nodes must be executed in accordance with the contract, and the violation of the agreement shall be punished by the rules. Intelligent contract monitors the operation of network nodes and verifies the operation behavior. It can be used to establish trust mechanism and discover and track abnormal behaviors in wireless terminals. The intelligent contract model is shown in Figure 2.

3. Challenges of Wireless Terminal Security with the Application of Block Chain Technology

With its inherent advantages of distributed storage, de-centralization, de-trust, data tamper-proof, block chain is suitable for applications in the field of wireless terminal equipment security. However, due to the limitation of hardware resources of most wireless sensor terminal devices, the direct application of block chain technology is confronted with challenges that cannot be ignored, which are specifically shown in the following aspects.

(1) Low processing capacity of hardware equipment.

The realization of block chain consensus, the execution of intelligent contracts, encryption and authentication, etc. all require nodes with high data processing capacity and hardware devices with high memory, CPU and power supply. However, most wireless terminals, such as Bluetooth devices and wireless sensor devices, are mainly used for data perception and are not equipped with enough computing power.

(2) Limited storage capacity. As a variety of transactions proceed, the data stored in the block will constantly swell, and the small operation behavior will lead to the increase of stored data. The characteristic of block chain distributed storage puts forward higher requirement for the storage capacity of wireless terminal hardware.

(3) Wireless connection performance. The wireless terminal equipment, which establishes the connection through the wireless network, the data verification, the synchronization, as well as the node consensus reaches, will put forward the high request to the network connection bandwidth, the stability and so on.

4. Wireless Terminal Security Architecture on the Block Chain Technology

Most of the wireless terminal equipment has limited resources, which has the characteristics of decentralized topology structure and unstable mobile communication. The emerging block chain technology has similar decentralized topology structure and features such as de-trust, tamper-proof and high reliability. Based on the block chain technology, this paper studies key technologies at all levels and proposes a wireless terminal security technology system on the block chain to provide security and feasibility assurance for wireless terminals. The structure is shown in Figure 3.

4.1 Definition and Lightweight Algorithm of Data Structure

In the data layer, all kinds of request behaviors of wireless terminals are instantiated and defined,

and lightweight hash algorithm and asymmetric encryption algorithm are adopted to improve computing performance. Traditional hashing algorithm includes SHA, MD 5, etc., weighing safety and efficiency, MD 5 can guarantee a certain security and is faster than SHA, so MD 5 hash function can be used for hashing calculation. Asymmetric encryption algorithm based on elliptic hyperbolic curve, is more widely used in practical environment to ensure the security of block due to its advantages such as small computation, small storage space and low bandwidth requirements.

4.2 Distributed Point-to-point Communication Network Model

For wireless sensor terminal devices with certain computing capacity and storage capacity, the network model is shown in Figure 4. Point-to-point connection is established between wireless terminals, and each terminal device carries transaction data and stores relevant keys to participate in data processing and forwarding. However, in the practical application, not all wireless terminals have powerful storage and computing power. For wireless terminals with limited hardware resources, they do not store transaction data or conduct data processing, but only collect sensor data and forward them. However, the nodes with strong computing power in a network can store and process the data. These wireless terminals store keys to ensure the security of data communication and forward the collected data to the nodes with strong computing power for data processing.

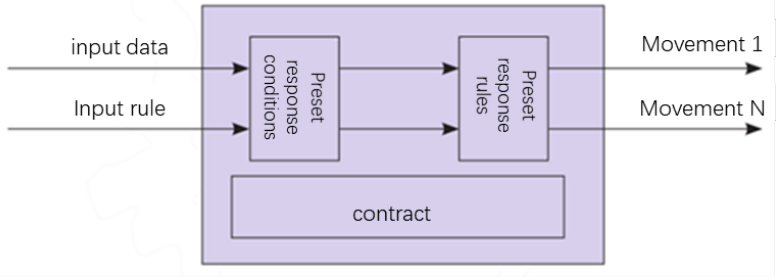

Fig 2 Intelligent Contract Model

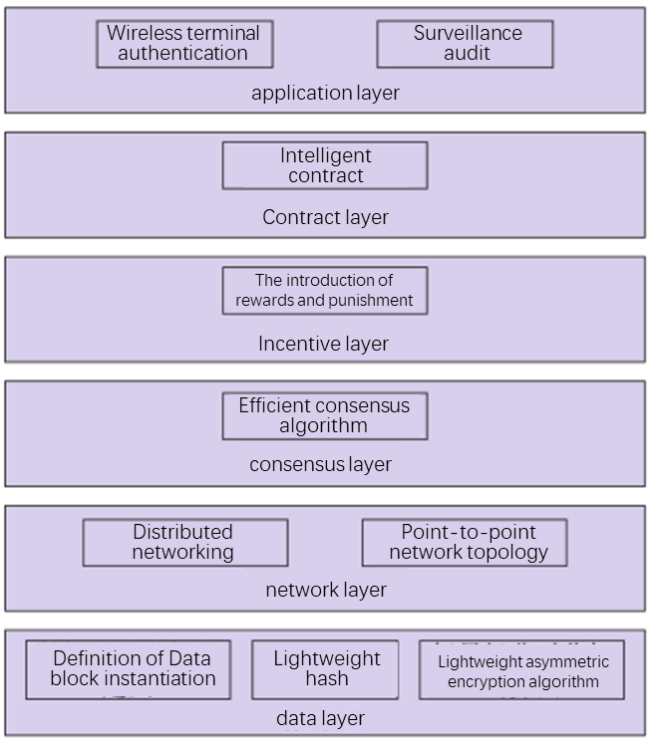

Fig.3 Wireless Terminal Security Structure on Block Chain

4.3 Efficient Consensus Mechanism

Consensus algorithm mainly solves the problem of obtaining consensus on transaction data in distributed network composed of distrust nodes. In a wireless network with block chain, when a

new terminal joins the network, the hash value of the previous terminal node must be used as the identity to complete the authentication. When multiple terminals join the network for authentication at the same time, it is necessary to improve the performance of consensus algorithm to improve the synchronization speed and thus improve the efficiency of block chain authentication. Based on the above requirements, firstly, the integrity and correctness of data should be ensured. And secondly, the consistency of transaction data confirmed in all consensus nodes should be realized [7]. The block chain consensus algorithm is the key to solve the above problems in the case of nodes with malicious tampering with data in the network and without a central node to be trusted.

First, a point-to-point distributed network. Once a node joins or exits, the consensus algorithm must be able to timely sense, adjust the structural parameters, and dynamically adapt to the network environment. In addition, when the computing resources (CPU, memory and bandwidth) of the network are reduced, its performance cannot be reduced rapidly. Instead, it needs to transition smoothly, so that the consensus algorithm can dynamically adapt to the resources, and the performance will not decline too much with the decrease of the number of resources.

Second, take handling capacity and latency into consideration. Combining with the existing authorization mechanism of consensus algorithm, and introducing the voting mechanism of consensus representative with reward and punishment mechanism, it maximizes the number of operational requests that can be processed per unit of time and reduce the time consumed by a single request.

Third, quantify the device status information. The effect of network change on device state is fully considered, and the influence of different quantization precision on the convergence speed of the algorithm is analyzed by quantizing the equipment state information.

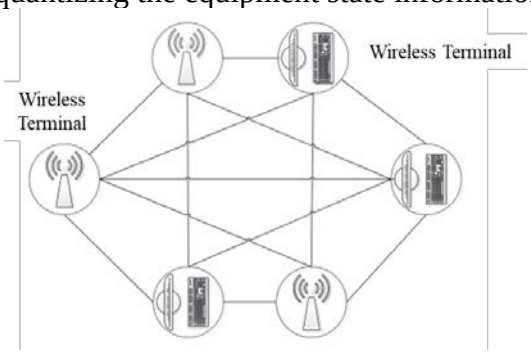

Fig. 4 Network Model

5. Conclusion

This paper provides a new method to solve the security problem of wireless terminal by analyzing the characteristics of wireless terminal and unstable network. At present, the academic research on blockchain has also made some achievements. Due to the short research time, the research on wireless terminal security is still based on the basic theory research. How to take into account the security and performance, and put the blockchain technology into practical wireless terminal security to provide better services is the direction of current researchers to explore.

Acknowledgement

This work was supported by Chongqing Yongchuan District Social Livelihood Science and Technology Special Project (Ycstc. 2018cc0301).

References

[1] HE Yu-jun, GONG Guo-cheng. A Summary of Research on Block Chain Technology in the Security Field of IoT[J].Telecom Engineering Technics and Standardizati on,2017,30(05):12-16.

[2] Sun Limin, et al. Wireless sensor networks [M]. Beijing: Tsinghua University Press Society,

2005

[3] SHEN Xin, PEI Qing-qi, LIU Xue-feng. Survey of BlockChain[J].Chinese Journal of Network and Information Security,2016,2(11):11-20.

[4] Sha Yi tian, Li Tian yi, Jia Wei. A Verifiable multi-party quantum key distribution protocol based on tree network[J]. Computer Applications and Software, 2019, 36(8):78-81