A Summary Research on the Security of IoT Based on Blockchain Technology

Dayong Ren, Jing Wang, Guojian Cheng
School of Intelligence Science and Information Engineering
Xi'an Peihua University, Xi'an, China
53908775@qq.com, 369607673@qq.com, 1683939013@qq.com

Keywords: Blockchain; Distributed Computing; De-centering; IoT Security

Abstract: The development and application of IoT has achieved remarkable results in recent years. A large number of sensors are connected to the machines and are combined with the Internet, which achieves intelligent management and operation. At the same time, the security and privacy problem in the IoT environment is still the one of the threats to the IoT technology. Because of the topology of the IoT as well as the constraint of resources, the traditional security technologies are not entirely applicable to the IoT.As the basic technology of bitcoin, blockchain technology has the haracteristics of decentralization,detrust, data encryption and so on. It is suitable for building a distributed system. This paper expounds the advantages of the blockchain technology in the network security, Put forward several directions for the application of blockchain to the security of IoT, which aims to help the research of blockchain technology in the security field of IoT.

1 Introduction

Blockchain technology is the core technology of digital encryption currency bitcoin representative system, it can be used for encryption, timestamp and consensus mechanism to realize distributed architecture, which is independent of any trust mechanism to the center, traceability, time stamp and digital signature can not be tampered with, guarantee open and transparent, can be regarded as a traceable bulletin board maintained by the nodes in the network in a distributed manner. Based on blockchain technology, Satoshi Nakamoto first proposed and standardized the concept of Bitcoin in 2008. With the rapid development of peer-to-peer transactions that do not pass through financial institutions, the concept of Bitcoin also starts with the earliest figures. Currency derives from a decentralized digital currency payment system. The Bitcoin network system generates new bitcoins in the form of computers that solve complex mathematical problems (which can be referred to as "mine mining"). Blockchain technology, as the core information technology in the Bitcoin transaction system, realizes a trust-free consensus network system by solving the double consumption problem and General Byzantine issue.

The IoT is the third wave of information after computer, Internet and mobile communication network. It is one of the strategic emerging industries which is listed as one of the most important development in China. Many policies have been promulgated by the country, and it is clear that we should effectively promote the construction of the IoT. There are some common features between IoT intelligent devices and bitcoin. For example, the network structure for P2P network, and there is no public infrastructure enough. In addition, all nodes are self-organizing. They can be records (for example, transactions or messages) that are broadcast to nearby nodes. The security of the IoT has been criticized, Major Internet Security Threats As shown in Fig.1. the blockchain can provide the best solutions for convergence with the IoT. Blockchain technology can provide trust, transparent and secure communication guarantee for the IoT, and establish an IoT authentication mechanism through the de centralized consensus mechanism to improve the security and privacy of the IoT.

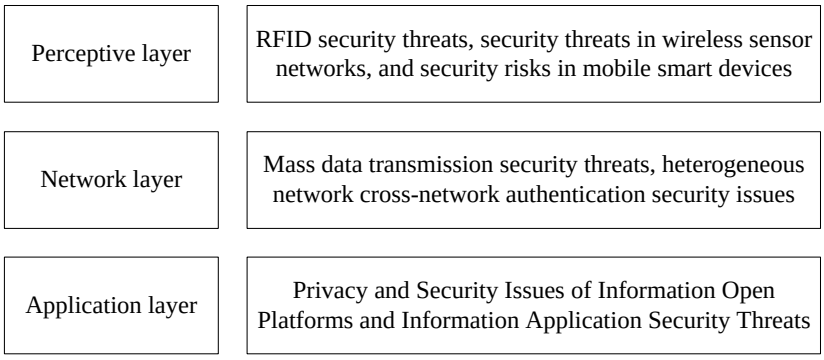


Figure 1. Major IoT security threats

2 The Main Security Issues in the Development of the IoT

2.1 Privacy Protection

The traditional IoT has many deficiencies in terms of user privacy and information security transmission: 1) The tag is embedded in any item, and the user is exposed to personal privacy without being aware of it; 2) The RFID system tracks the item and the privacy is compromised. 3) The detailed information of the item is transmitted between the local information server (L-TIS) and the remote information server (R-TIS) and is vulnerable to traffic analysis.

Traditional channel security cannot meet the needs of application-based privacy protection against key sharing attacks in "one-to-many" and "many-to-many" environments. Mobile intelligentphones embedded in GPS, WiFi, and other positioning devices expose users' location privacy. In public places. U.S. Sense Network handles more than 4 billion location data every day to extract user privacy, habits and other privacy information. Whether RFID devices, infrared sensors, mobile internet devices, and GPS positioning systems can completely protect the privacy data of users, whether or not these information are monitored by manufacturers are important issues that the security of the IoT needs to face.

2.2 Authentication and Access Control

There are two main types of authentication in the network: identity authentication and message authentication. Identity authentication is ensured by a key. If one of the two parties in the communication is stolen, the session data of both parties will be stolen by the attacker, causing loss of both parties. Message authentication is an authentication method used by senders and receivers to ensure the security and integrity of information during communications. The authentication in the IoT refers to a message authentication code when the sender and the receiver determine the communication, and the sender confirms that the receiver has received the message it has sent according to the message authentication code of the returned information. However, in the communication process, the message authentication code is generally static data, and the attacker can pretend to be a receiver to obtain the information sent by the sender through methods such as exhaustive data flow monitoring and the like, and the message authentication code of the returned information received by the sender. It is also correct. This will lead to security problems such as information disclosure in the IoT.

Access control refers to controlling access to certain resources according to authorization policies, thereby reducing the intrusion of illegal users and ensuring legal access to resources. At present, the access control mechanisms of information systems are mainly Role-based Access Control (RBAC) and its extended model. Guaranteeing information security during access control is a major security issue in the development of the IoT.

2.3 Data Security

The traditional database system deals with discrete data and the IoT deals with streaming data. Streaming data is real-time and continuous. Once attacked, all streaming data information will be stolen. With the combination of big data and the IoT, the storage and processing of massive data in the IoT is facing huge security challenges. As shown in Fig.2, the IoT acquires data through sensors

and is stored in databases such as MYSQL and ORACLE. The storage of other unstructured data is implemented through HDFS, GFS cloud storage, and so on. Cloud storage is a commonly used storage method at present, but the data needs to be transmitted repeatedly when it is used, causing the load of the central cloud server to be extremely large, and the security of the data is not guaranteed. The IoT applications need to consider data security and privacy, especially in the wireless IoT process, to prevent data from being used by unauthorized users.

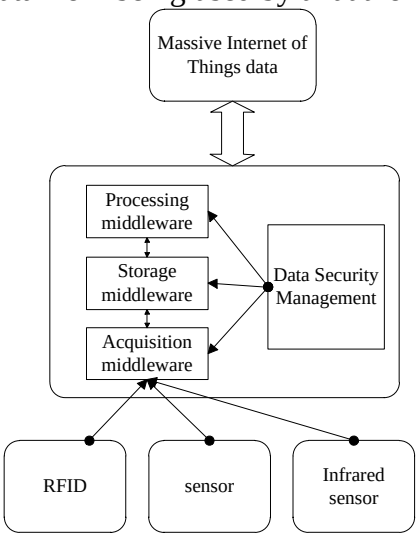
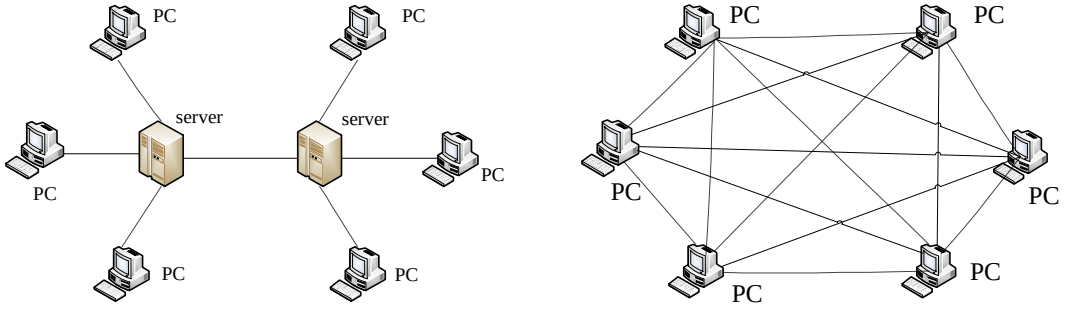


Figure 2. IoT data storage and processing structure

3 Blockchain Security Technology Analysis

3.1 Decentralized Topology

The most typical feature of blockchain technology is decentralization, which is also the most widely used feature in IoT security. In a blockchain network, there are no centralized nodes or management structures, and a large number of nodes form a decentralized network, as shown in Fig.3. The security maintenance of various functions in the network depends on all nodes in the network with security maintenance capabilities. There is no management mechanism between nodes, and each node is equal. Each node has a record of the complete database information. When a node receives data from another node, the node verifies the identity of the other node. If the verification is successful, it will The information it receives is broadcast to the entire network. Data verification, storage, maintenance and transmission in blockchain networks All of them are based on distributed system architecture. Mathematical methods are used instead of central agencies to establish trust between nodes. Therefore, blockchain technology has a better optimization effect on the central structure of the IoT. The use of blockchain decentralization can improve the existing state of centralized data storage and the centralization of the IoT structure, reduce the dependence of the IoT on the central structure, and prevent the collapse of the entire system due to the damage of the central structure.



a) Centralization network

b) De centralization network

Figure 3. Comparison between centralized and decentralized networks

3.2 Blockchain Structure

A blockchain consists of a block and a chain structure, which can effectively prevent the change of transaction information of a certain block and control the generation of new blocks. Block is the network node of the blockchain. It is a data structure for recording transactions. Each block consists of a header and a body. The structure is shown in Fig.4.

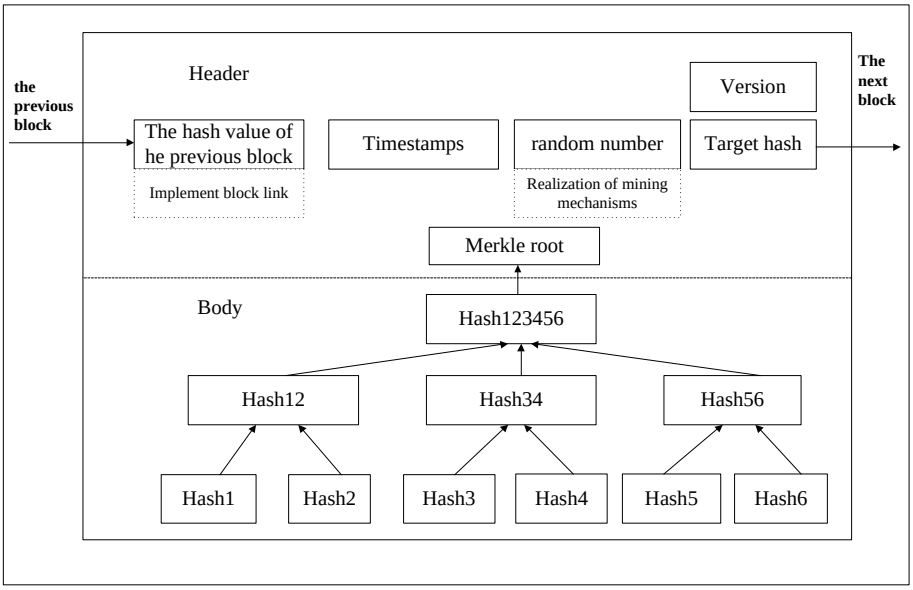


Figure 4. Blockchain structure

The block header contains all the information except the transaction information, in which the Hash Used is used to connect the block with the previous block, forming a chain structure; the time stamp is responsible for recording the time generated by each block; Merkle root summarizes all transaction information in a block, and finally generates a unified hash of all transaction information for this block. This value changes with the transaction.Change to produce changes, by dynamically adjusting the difficulty value of the target number; the miner who first finds the correct solution to the correct number (the Nonce) will get the current block accounting rights. The block body is only responsible for recording all transaction information within a period of time. The transaction information is task data carried by the block, and specifically includes the private key of the transaction parties, the number of transactions, digital signature of the electronic currency, etc.

3.3 Asymmetric Encryption Algorithm

The asymmetric encryption algorithm is an encryption method consisting of a pair of unique public and private keys. A public key and a private key are a pair. If the data is encrypted using the public key, only the corresponding private key can be decrypted; if the data is encrypted using the private key, only the corresponding public key can be decrypted. In the Bitcoin system, the private key is a random number, a public key is generated by an irreversible encryption function, and a bitcoin wallet address is generated using a hash function through the public key, as shown in Fig.5.

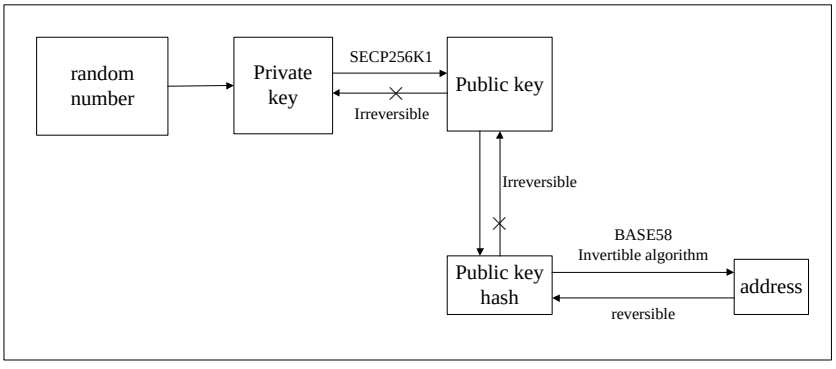


Figure 5. Asymmetric encryption algorithm

3.4 Consensus Mechanism Technology

The consensus mechanism technology is another basic technology in the blockchain. The consensus mechanism is used to determine the accounting nodes in the blockchain network and to confirm and synchronize the transaction information. At present, the consensus mechanism that people research and adopt is mainly the proof of work (POW), which takes the computational cost needed to solve the difficult problem as the vouchers for newly added blocks and obtain incentive income.

The basic idea of POW is to set up an incentive mechanism (reward a certain amount of digital currency) to attract nodes in the blockchain network to make a SHA256 mathematics problem that is difficult to solve but easy to verify. The math problem requires the calculated random number. Less than or equal to the target hash value, the random number that meets the requirement usually consists of multiple leading zeros. If the target hash value is smaller, the difficulty of finding the random number is greater. To find this random number requires a lot of computing power. Some nodes attempting to change existing blockchains need to invest more computing power to recalculate. This situation is still only theoretical, and as the height increases, the required computing power increases geometrically. This mechanism ensures the data consistency of the blockchain and cannot be modified, but at the same time it also brings about waste of resources, and even loses the advantage of decentralization due to the emergence of super large mining pools.

3.5 Intelligent Contract

The intelligent contract encapsulates a number of preset response conditions, trigger conditions, and operations. The parties to the contract agree on the content of the contract and deploy it on the blockchain in the form of code. When certain trigger conditions are met, the intelligence is activated automatically. The contract is executed and its model is shown in Fig.6. Intelligent contracts play an important role in the development of blockchains, providing them with broader Prospects. Applied to the IoT, intelligent automation can be realized in many areas such as intelligent agricultural systems, intelligent homes, and intelligent power, such as automatic temperature and humidity control, remote power meter reading, and so on.

From a security point of view, intelligent contracts first have the same characteristics as common blockchain data, distributed, documented, consistent, and irrevocable to delete. Second, intelligent contracts are also used as a guarantee of blockchain security. Technical means. In the intelligent contract, the rights and obligations of the participants, the triggering conditions of the contract execution, and the corresponding results are defined. Once the intelligent contract is added to the blockchain, it can be executed objectively and accurately without being affected by either party.

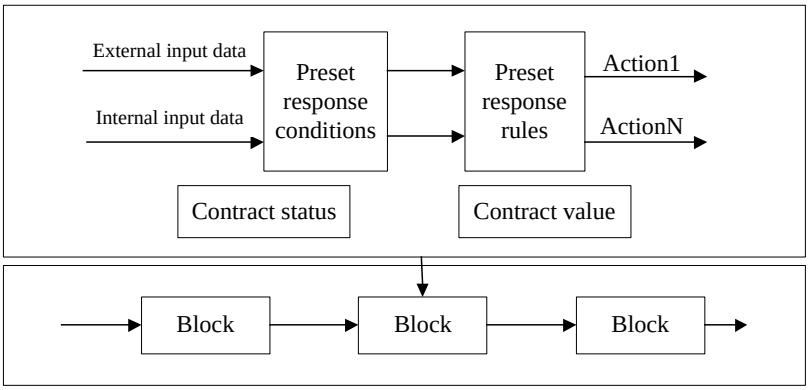


Figure 6. Interlligent contract model

4 The Application of Blockchain Technology in the Security of IoT

4.1 IoT Intelligent Device Key Update based on Blockchain Technology

At present, the IoT intelligent device uses the identity-based encryption algorithm IBE, which can use the user's identity as the public key for encryption or signature verification. To ensure that the public key does not lose due to security problems, and to prevent replay attacks, the user's

public key Need to be updated regularly. To solve this problem, use the blockchain technology to update the key. The user will use his identity as the public key during the initialization phase and obtain the corresponding private key through the PKG (private key generator). Then, the user can randomly generate a new private key and generate the corresponding public key through an algorithm. Since this public key is a random number, the user will publish this change to the blockchain, and all other users can see it. With this change, the latest public key corresponding to the user's identity can be found through the blockchain. In this way, the latest public key is used in all subsequent encryptions.

4.2 Trusted Location Technology based on Blockchain

In the absence of positioning signal, intelligent IoT equipment using the relative position of all devices in the network positioning scheme based on APS, as shown in Fig.7, a landmark building in O, B and C three, the mutual distance between three points is known. If the equipment between A and three landmarks building distance can be determined, the system can calculate the relative position of A equipment; if the equipment can only be identified with the landmark B, C distance, according to the equipment A or a two possible position, with the addition of other devices in the network or landmarks, the exact location information of the voting mechanism can be calculated by A the simulation results show that the positioning accuracy and measurement accuracy of the distance between the nodes, and increased with the increase of GPS signal, with auxiliary positioning function in the GPS signal under the condition of weak. Each device publishes the acquired peripheral device names and distances in the blockchain network. After obtaining the distance information published by each device in the network, the miners can use the Euclidean distance algorithm to calculate the various intelligent devices in a no-position signal environment. The mutual position, thus calculating the overall relative positioning of all intelligent devices in the entire network, if the weak positioning signal or characteristic landmark conditions, the positioning accuracy will increase as the signal strength increases or the number of landmarks increases. Under the consensus mechanism, only valid information of each device can be disseminated and published in the blockchain. Therefore, a user attempting to falsify a positioning location cannot obtain approval from most intelligent devices around its forged location, so its location information cannot be Propagation cannot be calculated by the miner and published in the blockchain. Therefore, this solution can effectively solve the problem of positioning in the absence of positioning signals or weak positioning signals, and make the location information issued by each device in the network be trusted.

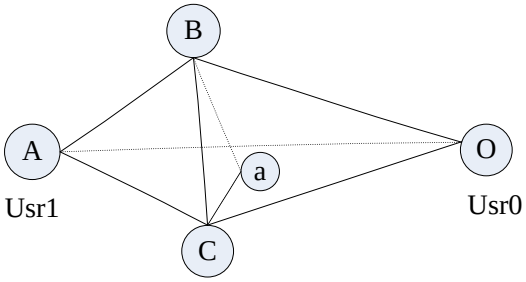


Figure 7. Ad hoc positioning system

4.3 IoT Intelligent Device Authentication

When an IoT device accesses the network, it needs to authenticate the device and confirm the identity of the device. The IoT can apply the idea of blockchain technology, adopt asymmetric encryption algorithms and intelligent contracts, and use the network device nodes in the P2P network to authenticate access devices, and the IoT devices only need to connect to the IoT platform and network devices. The node sends the access and authentication request to authenticate and connect the IoT device to the IoT platform. Applying blockchain technology to IoT device authentication without the help of third-party devices can effectively reduce the cost of authentication, improve the security of IoT devices, prevent illegal device masquerading, and protect the device from external attacks.

4.4 Constructing the IoT Consensus Network

By revising the consensus verification mechanism of the blockchain, a consensus network applied to the IoT can be constructed. In the IoT environment, intelligent device nodes do not assume data calculation work, do not participate in the workload mechanism proof, only encrypt and transmit data, and broadcast data transmission to the entire network as blockchain transactions. In addition, specific verification nodes are deployed to perform POW calculations, verifying that nodes do not save transaction data, and play a role in data security and privacy protection.

4.5 IoT Intelligent Device Tracking

Blockchain technology can create a new way to track the unique history of a single device by recording the account books of data exchanged between the device and the user or network service. Blockchain can also make intelligent devices stand-alone agents and manage transactions individually. For example, connecting a vending machine can track the user's purchase history and use this to automatically pay for new items delivered. Through device tracking, real-time understanding of the device's use status, once an exception occurs, immediately respond to the maximum protection of the device security, thus ensuring the security of the entire IoT network.

5 Conclusion

With the development of the IoT and blockchain technology and the reliance of the industry on the IoT, the blockchain technology will be more applied to the IoT, and can establish a low-cost direct communication between the mass of the IoT intelligent devices. at the same time, through the decentralized consensus mechanism, improves the efficiency of intelligent device key updating and the credibility of the positioning. Based on intelligent contracts, the intelligent device becomes an independent entity that can be self-maintained and adjusted, facilitating the implementation of intelligent devices. Track management to improve the security and usage of intelligent devices. The IoT enhances the connection between things and things, and blockchain provide security for such connections. For the more effective use of blockchain for IoT security, deeper levels of research and exploration are needed in the future.

References

[1] Zibin Zheng, Shaoan Xie, Hongning Dai. 2017. Blockchain Challenges and Opportunities:Asurvey [EB/OL].https://www.researchgate.net/publication/310328910_Blockchain_Challenges_and_Opportunities_A_Survey.

[2] CHRISTIDIS K, DEVETSIKIOTIS M. 2016. Blockchains and Intelligent Contracts for the IoT[J].2016 (4):2292-2303 IEEE Access.

[3] Nakamoto S. Bitcoin, 2009. A peer-to-peer electronic cash system[J].Consulted.

[4] Melanie Swan M. Blockchain 2015.blueprint for a new economy[M]. USA：O'Reilly，

[5] Antonopoulos A M. Mastering Bitcoin 2015. Unlocking Digital Crypto-Currencies[J]. Oreilly Media Inc Usa,

[6] S Li，LD Xu，S Zhao. 2015. The IoT: a survey[J]. Information Systems Frontiers:2015,17(2):243-259.

[7] STULMAN A, STULMAN A. 2015.Spraying techniques for securing key exchange in large ad-hoc networks[C]. In:Proceedings of the 11th ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet 2015). ACM, 29–34.

[8] CHATURVEDI A, SRIVASTAVA N, SHUKLA V, et al. 2015. A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks[J]. International Journal of Computer Applications,2015, 128(2): 36–39.

[9] BÜTTNER C, HUSS S A. 2015. A novel anonymous authenticated key agreement protocol for vehicular ad hoc networks[C]. In: Proceedings of the 1st International Conference on Information
Systems Security and Privacy—ICISSP 2015. SciTePress, 2015,259–269.

[10] NICULESCE D, NATH B. 2001. Ad hoc positioning system (APS)[C]. In: Proceedings of the Global Telecommunications Conference—GLOBECOM 2001.IEEE, 2926–2931.

[11] KOSBA A E, MILLER A, SHI E, et al. Hawk.2016. The blockchain model of cryptography and privacy-preserving intelligent contracts[C]. In: Proceedings of IEEE Symposium on Security and Privacy—SP 2016. IEEE ComputerSociety,:2016, 839–858.