Research on the Key Technology of Safety Protection in Application Environment of Blockchain

Hua Zhang, Jiong Wang, Ge Xu, Zhiqiang Ruan.
College of Computer and Control Engineering, Minjiang University, Fuzhou 350108, China
Fujian Provincial Key Laboratory of Information Processing and Intelligent Control (Minjiang University)
First author: Hua Zhang
Corresponding author: Jiong Wang

Abstract: This paper analyzes the current situation of blockchain application security. Then, makes a concrete analysis on the problems existing in the application safety of blockchain, including the attack of consensus algorithm, the leakage of privacy, and the programming vulnerability of blockchain and hash collisions. Then it introduces in detail the three key technologies of security protection under the blockchain application environment, P2P network technology, asymmetric encryption technology and consensus mechanism technology. In order to make more relevant people know more about the key technologies of safety protection in the application environment of blockchain.

1. Introduction:
The product of the development and progress of computers is the block chain, which adopts encryption algorithm, point-to-point transmission, sharing mechanism, distributed data storage and other computer technologies, and effectively solves the problem of traditional single-party control and modification of electronically stored data through technical means and mathematical methods. In other words, the block chain brings all participants together to establish an effective trust mechanism. If the block chain is regarded as a public account, the account needs to be jointly maintained and supervised by the participants. Users save their own operation time and identity on the account while recording. The data information of the account can be consulted by the participants at any time, and its information cannot be deleted or modified, thus establishing a trust platform for all participants.

2. Current Situation of Application Security of Blockchain
At present, the advanced and advanced computer technology of regional chain has been widely applied in intelligent tourism, entertainment and games, financial securities, commodity production and logistics transportation. In many aspects, the application of block chain technology has achieved remarkable results. The advanced technology of block chain provides a new way of development for sharing, intelligence and informatization in different fields in the society, but at the same time, the application safety of block chain also needs to be paid attention to.
3. Problems existing in Blockchain Application Security

3.1 The attack of consensus algorithm
As we all know, one of the advantages of block chain technology is decentralization. Different network nodes can maintain their own backup of block chain ledger, but sharing records with other nodes requires consensus algorithm to be implemented through consensus nodes in all networks. At present, the node that most nodes jointly maintain is the correct block chain book recognized on the network. The so-called attack means that the workload proof calculation method exceeds 50% (51% and above). In other words, if more than 51% of the block chain is mastered and the normal block chain is transferred to the illegal block chain, the nodes of the whole network will be transferred to work on the illegal block chain. Even with the continuous improvement of security technology, 51% of force attacks are still potential security risks.

3.2 The leakage of privacy
At present, financial banks are widely used in block chains, such as some digital cash such as Bitcoin. Different nodes in the network can intuitively obtain different information and data in the block chain. In order to effectively protect the privacy information of the block chain, Bitcoin usually uses random number to generate addresses and asymmetric encryption algorithm to "hide" the user's real identity information. However, because the address information is closely related to the user's real information, it cannot completely protect the user's privacy information and may also cause the problem of privacy disclosure.

3.3 The programming vulnerability of block chain
Under normal circumstances, in the practical application of block chain, mathematical method is a means of building trust relationship between block chain technology. In the process of writing more complex application programs, programmers cannot have perfect programming language and mathematical logic. In other words, the programmer's algorithm for writing application programs is not impeccable, which is also an important potential safety hazard in block chain programming.

3.4 Hash collisions
According to the hash algorithm, the unique identifier of the chain of blocks that are linked together by values is the hash value, and one of its characteristics is that it cannot be tampered with. If the same hash value is constructed in data blocks with completely different contents, it is very likely to seriously tamper with the data blocks. If multiple different nodes are generated to tamper with the hash value at the same time, it will make it difficult to distinguish different data blocks, resulting in a block chain that cannot be better used.

4. The key technologies of security protection under the blockchain application environment

4.1 P2P network technology
One of the key technologies that can make the block chain run stably is P2P network. The characteristics of P2P network include privacy protection, load balancing, strong fault tolerance and de-centralization. If the network of the block chain designs the minimum world model according to the security requirements of P2P, the network can be divided into candidate accounting nodes and non-accounting nodes according to the type of node selection whether accounting is performed, the candidate accounting nodes are used for privacy information recording, and the non-accounting nodes are used for transaction activity verification. After continuous improvement and development, the third generation structured P2P network mode has been developed to reduce the total probability of block chain computation, effectively reduce the amount of information sent, cancel the flooding algorithm, and quickly locate problems. The small world model P2P network structure is as follows: Fig. 1
The whole network consists of all clusters, and nodes on the network can form different clusters. Different clusters consist of a cluster head node and several ordinary nodes. The cluster head node changes according to other random factors and the node's capability contribution, such as node change, node exit and join, etc. At the same time, the number and role of nodes in the cluster also change dynamically with the change of the cluster.

4.2 Asymmetric encryption technology
One of the important guarantees for the application security of block chain is asymmetric encryption, which includes two key keys, private key and public key. The private key refers to a string of fixed-length character strings generated according to SHA256 hash algorithm or Base58 conversion algorithm, and then the private key is changed into a public key whose generation process is irreversible through another algorithm. At this time, SHA256 hash will generate 2256 private keys that are difficult to crack due to current block chain calculation. Asymmetric encryption technology is mainly applied to digital signature and data encryption in block chain. In the process of data encryption by digital signature, A represents the sender of the information and B represents the receiver of the information. At this time, A uses B's public key to encrypt the information it sends, and then sends the processed information to B. At the same time, B uses its own private key to decrypt the data in the process of obtaining the original information. This is the application of asymmetric encryption in the whole transaction information of the block chain. As shown in the following figure, the transaction of the block chain can be divided into two parts. Transaction signature: the public key of user 2, the recipient of transaction 2, encrypts transaction 1 with hash, and user 1 needs to use its own private key to sign the hash in the previous step; Transaction verification: user 1 uses the public key to decrypt its signature so as to obtain X information, while the data of the last transaction is spliced with user 2 and hash operation is carried out using the same method so as to obtain Y information. If Y is equal to X at this time, user 1 can be verified as the sender and user 2 as the receiver, which also indicates that this transaction is carried out between user 1 and user 2. This process also reflects the authenticity and secrecy of the block chain by applying asymmetric encryption technology in the block chain, shown in Figure 2.
Consensus mechanism is also crucial in the application of block chain. Consensus mechanism confirms transaction information in block chain and decides accounting nodes in block chain network, which ensures the consistency of data in block chain. The publicity mechanism not only introduces the share authorization certificate, but also introduces the theories of rights and interests certificate and workload certificate. The share authorization certificate can select some representatives to obtain income from the equity certificate; Proof of rights and interests is also a substitute for proof of workload. The highest point of rights and interests realizes it and completes the addition of new blocks at the same time. The workload proof can solve the problem of difficult calculation in the block chain, and at the same time the cost of settlement can be used as the incentive income and the newly added block voucher. Consensus mechanism can ensure the security of the network and effectively resist attacks in the network. The huge cost of carrying out the attack makes illegal personnel flinch, thus reducing the probability of being attacked.

5. Conclusion:
All computer information technologies need to face attacks from viruses, trojan and hackers, and block chains are no exception. In the face of these real-time and dynamic security problems, the block chain needs to adopt asymmetric encryption technology, P2P network technology, consensus mechanism and other technologies, as well as DDOS attack prevention technology, ciphertext access control technology and key management technology to effectively avoid key loss and further promote the development and popularization of the block chain.

Acknowledgment
This work was supported in part by the Education and Research Project for Young and Middle-aged Teachers in Fujian Province in 2018 under Grant JT180405, Fujian Provincial Key Laboratory of Information Processing and Intelligent Control (Minjiang University) under Grant MJUKF-IPIC201809), Fuzhou Science and Technology Plan Project under Grant 2017-G-106, and the National Nature Science Foundation of China under Grant 61871204.

References:
[1] Han Xuan, Yuan Yong, Wang Feiyue. Blockchain Security Issues: Current Situation and Prospect[J]. Acta Automatica Sinica, 2019, 45(01):206-225.
[2] He Haiwu, Yan’an, Chen Zehua. Overview of Intelligent Contract Technology and Application Based on Blockchain[J]. Journal of Computer Research and Development, 2018, 55(11):2452-2466.
[3] Peng Jinjie, Long Ruolan. Research on Key Technologies of Security Protection in Blockchain Application Environment[J]. Network Security Technology and Application, 2018(06):26+33.
[4] Chen Dai. Research on Key Technologies and Application Schemes of Cloud Computing Based on Block Chain[D].Xidian University,2018.

[5] Han Shuang. Research on Security Control System of Voucher Based on Block Chain Technology[D].University of Chinese Academy of Sciences（Shenyang institute of computing technology, Chinese academy of sciences）,2018.

[6] Zhou Liangjin. Research on Railway Passenger Privacy Protection Technology Based on Block Chain and Distributed Database[D].China Academy of Railway Sciences,2018.

[7] Zhou Zhicheng. Research on Key Technologies of Cross-domain Authentication for Large Data Security Applications Based on Block Chain [D]. Information Engineering University,2018.

[8] Zhu Yan, Gan Guohua, Deng Di, Ji Feifei, Chen Aiping. Research on Security in Key Technologies of Block Chain[J].Journal of Information Security Research,2016,2(12):1090-1097.