Identity Management Security Authentication Based on Blockchain Technologies

Pengfei Fan[1], Yazhen Liu[1], Jiyang Zhu[1], Xiongfei Fan[2], and Liping Wen[3]
(Corresponding author: Pengfei Fan)

Information Communication Operation and Maintenance Center,
Information and Communication Branch, State Grid Inner Mongolia Eastern Electric Power Co., Ltd.[1]
Training Center, Inner Mongolia Power (Group) Co., Ltd.[2]
Hohhot Power Supply Bureau, Inner Mongolia Power (Group) Co., Ltd.[3]
Hohhot, Inner Mongolia Autonomous Region 010020, China
(Email: lyzfpf@126.com)
(Received Sept. 22, 2018; Revised and Accepted June 12, 2019; First Online Oct. 1, 2019)

Abstract

In recent years, the popularity of the Internet and computers has made people's communication more convenient and faster, and access to information has become faster and faster. However, due to the openness of the Internet, how to ensure the legal and credible identity in the communication process has become an important part of Internet security. This study briefly introduced the block chain and the block chain-based identity security authentication system and simulated and analyzed the block chain and security of the system. The results showed that the block chain could accurately authenticate the user identity information of the input public key after issuing valid digital certificate and prevent the non-authenticated identity information user from viewing the digital certificate. The increase of block chain nodes also increased the fault-tolerant nodes. At the same time, the endorsement conditions which were that the normal nodes were larger than half of all the nodes made the nodes of the system used safely as long as the number of damaged nodes was no more than half. The hackers needed to successfully attack more than half of the nodes before tampering the system data, but this operation was almost impossible to achieve objectively. Thus, the security of the system was extremely high.

Keywords: Block Chain; Digital Certificate; Identity Authentication; Smart Contract

1 Introduction

In recent years, the popularity of the Internet and computers has made people's lives more convenient [13]. The most intuitive one is the exchange and acquisition of information. However, the emergence of the Internet has not only brought convenience, but also brought information security risks. The Internet has openness and anonymity [7]. The former is an important factor in the development of the Internet. The latter has formed a hidden danger after combining the former. Users participating in the Internet cannot guarantee whether the communication object is trustworthy. Therefore, identity management has become one of the important technologies for Internet information security.

The basic principle of the identity authentication management technology [9] is to generate a unique digital certificate for the application user as the identity certificate. At the beginning, limited by technology, the identity management system is mainly a centralized system [11], which is that digital certificates and keys are provided by third parties, and identity information is also kept by third parties. The centralized identity authentication system protects the user's identity information to some extent, but it has obvious shortcomings and cannot guarantee the credibility of the third party, including termination of third-party service, data loss or malicious leakage of data. People's demand for identity authentication systems is not met until the emergence of block chain technology.

The important features of block chain technology [4] are decentralization and collective maintenance. The former is the same authority between nodes, while the latter is that all nodes share the identity information authentication, and the authentication process is transparent, open and credible. Yu *et al.* [14] proposed an effective social network information privacy protection algorithm, which used the block chain to store the user's public key and encrypted the plaintext by hybrid hash encryption algorithm after binding. The simulation results showed that the algorithm could effectively defend against different types of attacks. Lin *et al.* [8] proposed a block chain-based secure mutual authentication system, BSEIN, to implement an access control policy. The system could provide privacy protection such as anonymous authenti-

cation, and the system had good scalability due to the smart contract of the block chain.

The performance evaluation results showed that the system's response speed was excellent. Guan *et al.* [15] divided users into different groups. Each group has a private block chain to record the data of its members and use pseudonyms to protect user privacy with Bloom filter for fast authentication. The experimental analysis showed that the method could meet the security requirements and the performance was better than other common methods. This study briefly introduced the block chain and the block chain-based identity security authentication system and simulated and analyzed the block chain and security of the system.

2 Blockchain

As shown in Figure 1, block chain has six block tables. The blocks from bottom to top are linked in chronological order on a cryptographic basis. Block chain technology adopts timestamp proofing, cryptography and other technologies, coupled with the distributed storage structure of the block to make the block chain decentralized and difficult to falsify forgery and collective maintenance, which ensures the security and privacy of important data in the block. At the same time, the block chain can also be regarded as a state machine that constantly changes its state through transactions. Its evolution formula [12] is:

$$\theta_{t+1} \equiv Y(\theta_t, T),$$

where θ_t represents the block chain state at time t, T is a transaction, and $Y(\cdot)$ is a state transition function. After the transaction has evolved for a period of time, the verified transaction is collected into the block, and the block is connected by hash value. The state conversion formula [2] is:

$$\begin{aligned} \theta_{t+1} &\equiv \prod(\theta_t, B) \\ B &\equiv ((T_0, T_1, \cdots), \cdots), \end{aligned}$$

where $\prod(\cdot)$ is a block B-based transaction conversion function, and the block B contains transactions T and other data.

In the view of structure, the data layer is the lowest layer, and the block encapsulates the basic unit as transaction data and uses cryptography such as Hash algorithm and encryption algorithm to construct the linked data in chronological order. The encryption algorithm is divided into two types: symmetric and asymmetric. The former encrypts and decrypts with one key, while the latter is divided into private key and public key. The derivation between the two is irreversible.

The network layer is the main manifestation of the decentralization of block chain. The content of its package includes network architecture, inter-block communication protocol and authentication method [5]. After a long period of development, the block chain usually adopts a point-to-point (P2P) network architecture. In this network architecture, the computer nodes participating in it provide the same service through the topology, so there is no central service in the block chain. The consensus layer encapsulates all the consensus mechanism algorithms between the nodes in the block chain. Due to the decentralization of the block chain, the "books" of each node are highly dispersed, thus, a consensus algorithm is needed to select the most suitable node to perform "billing rights." The process of running a consensus algorithm to select a node is called "mining." The commonly used consensus algorithms are: workload proof, equity certificate, entrusted equity certificate, *etc.* This study adopted the most secure consensus algorithm, workload proof [10], which is currently recognized.

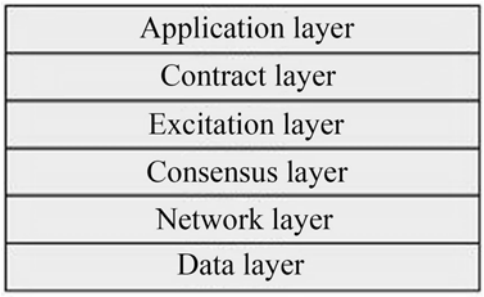

Figure 1: Framework of blockchain

The above data layer, network layer and consensus layer are the necessary and indispensable factors of the block chain. In addition, the incentive layer is used to reward the structure of the nodes involved in the "mining" of the block chain. It stimulates a large number of nodes to participate in "mining" through rewards, thereby realizing the stability and security of the block chain by means of consensus mechanism. The contract layer encapsulates a piece of contract code that is executed when the pre-defined conditions are met.

3 Blockchain-based Identity Authentication System

3.1 Overall Structure

As shown in Figure 2, the overall architecture of the block chain-based identity authentication system [1] is divided into three parts: an identity authentication system with primary functions, a third-party publicity module for inquiring, and block chain module for privacy security connected with two modules. The identity authentication system is a functional manifestation of the entire system, including a registration system, a certificate issuance system, a block chain management, and an SDK, and the registration system implements a traditional user identity

registration function.

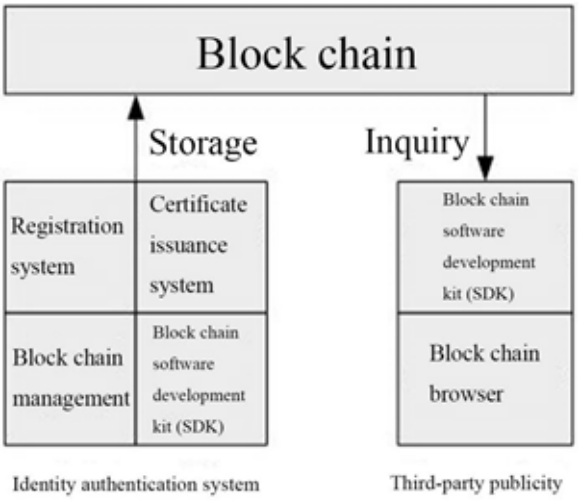

Figure 2: The overall structure of the identity authentication system based on the block chain security system

The certificate issuance system implements the traditional user identity authentication function, but unlike the traditional one, the module only has the function of issuing a certificate, and the specific digital certificate and related operation records are performed in the block chain. The main function of the block chain management module is to manage the nodes in the block chain, the consensus policy, the smart contract, *etc.*, and the authority for the management operation is only owned by the corresponding administrator, and the execution of the operation requires the consent of multiple parties to pass. The block chain SDK is responsible for connecting the authentication system and block chain, storing identity data operations into the block chain, and receiving information from the block chain.

The third-party publicity module is a module for system users, which includes a block chain SDK and a browser. The role of the SDK is similar to that of the SDK of the authentication system. The public module is connected to the block chain, and the operation information is input and the authentication information is inquired. A browser is a third-party platform that displays or inquires the authentication process, mainly referring to web pages.

The block chain is an important module for the privacy security of the system. This study used the callback function to form the smart contract [6]. The smart contract includes logical operations such as certificate storage and query, issuing key loss management, and certificate revocation management. The execution of a complete smart contract includes three steps of node signature, consensus calculation and accounting. At the same time, in order to improve the credibility of the smart contract call data, the contract can be executed when the node signature is not less than three.

3.2 Certificate Management

For the identity authentication system, the management of the certificate is a crucial part. The issuance, replacement and revocation of the certificate are related to the generation, change and cancellation of the user's identity rights in the system [3]. The most important certificate issuance process is shown in Figure 3. First, the user sends a certificate request to the registration center of the system. The content of the application includes the user digital certificate type, public key and public key validity period, and the information is unique. After receiving the application information, the registration center will automatically or manually review the information and send the certification license to the issuing center after the approval.

After receiving the certification, the issuing center generates a digital certificate according to the template. After receiving the certification, the issuing center generates a digital certificate according to the template. The certificate contents include the serial number and signature algorithm for proving the validity, the holder information for proving the ownership, the public key and validity period for protecting the privacy, and the information of issuer for proving the source. After the certificate is generated, the smart contract is called to verify it. After the signature algorithm is passed, the certificate is stored in the block chain to ensure that the identity corresponding to the digital certificate is transparent and cannot be falsified. After the block chain is successfully deposited, the information of successful operation will be fed back step by step, and the user will be notified by mail or telephone. Compared to traditional identity authentication systems, block chain-based authentication systems are initiated by the user side in generating keys for privacy protection. At the same time, the digital certificate generated by the formal route and stored in the block chain can be inquired through the block chain. When the inquiry cannot be operated, the certificate has expired or is leaked, and the certificate update or revocation is required, and the certificate issuance process is similar.

4 System Performance Test

4.1 Experimental Environment

As shown in Figure 4, the experiment was carried out on the primary server of the lab. The parameters of the primary server were quad-core i7CPU, 16G memory and 1024G hard disk. The Virtualbox software was used to divide two virtual machines (VMs) in the server. The configuration parameters were dual-core CPU, 2G memory, 40G hard disk, acting as the identity authentication system center. VM2 configuration parameters were dual-core CPU, 3G memory, 40G hard disk. 360 browser was used in the paimary server for registering and querying digital certificates in the authentication system of VM1, and VM1 and VM2 were connected by a block chain SDK. To

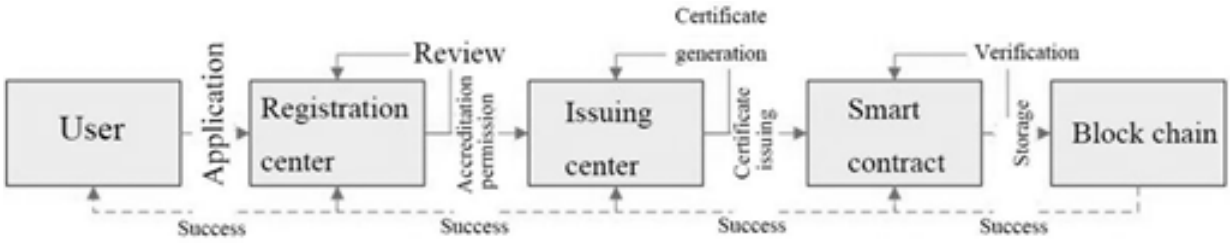

Figure 3: Process of certificate management

facilitate the simulation, the parameters of the nodes in the block chain network were uniformly set as single-core i5CPU, 2.5 GHz working frequency, and 4 G memory.

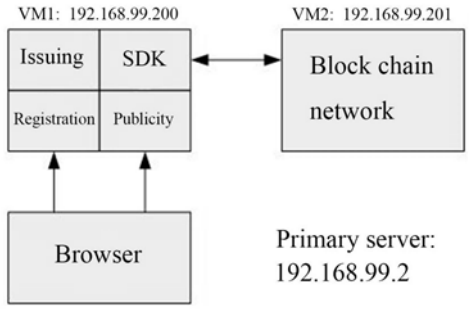

Figure 4: Structure diagram of system test based on blockchain

4.2 Test Content

4.2.1 Identity Authentication Test

Firstly, the user private key was generated by using the RSA algorithm in the Openssl tool. Then, the user public key was generated according to the private key, and the certificate was applied to the browser registration interface by using the public key. After the necessary identity information was successfully applied, the Openssl tool was used to randomly generate another private key and public key. Then, the two public keys were respectively applied through the block chain SDK to simultaneously inquire the three nodes in the block chain for the previously applied digital certificate, and the inquiry result was recorded.

4.2.2 System Security Test

First, three nodes were set for block chain, and two of them were verified, i.e., the operation could be performed when the node signature was not less than two. After that, a certificate was issued, and its validity was checked. When the certificate was invalid or not found, the identity information was leaked. One of the nodes was stopped to simulate the node being hacked, and the rest of the nodes worked normally as issuing or updating the certificate and inquiring the validity. Then, after another node was stopped, the operation of issuing or updating the certificate and inquiring the validity continued. When it was invalid, the next step was to resume the node work one by one and inquire the validity separately. The number of nodes was gradually increased in the block chain, and the number of nodes passing through was always kept larger than half of all nodes. For each additional number of nodes in the block chain, the previous steps were repeated to test the number of fault-tolerant nodes under different node numbers of the system.

4.3 Test Results

4.3.1 Test Results of Identity Authentication

Due to space limitations, only the public key used for the certificate application was listed. As shown in Figure 5, the public key had a length of 1024 bits.

As shown in Table 1, the three nodes with the correct public key for the digital certificate could pass the identity authentication. The random public key was used for the digital certificate inquiry, all the three nodes could not pass the identity authentication, and the interface showed that “There is no such certificate. Please inquire if your information is entered correctly.”, after it returned. It could be seen that the block chain could effectively authenticate the identity information of the valid digital certificate and prevent the non-authenticated identity information user from viewing the digital certificate.

4.3.2 Test Results of System Security

As shown in Figure 6, as the number of nodes involved in ”mining” in the block chain increased, the passing conditions of the system were constantly adjusted, and the conditions of more than half of all nodes were always maintained, and the number of fault-tolerant nodes was also rising. For example, when there were ten nodes in the block chain, the passing condition was six nodes, and the fault-tolerant node was four. This meant that even if four nodes in the block chain were abnormal due to hacking, a bad inquiry signature was issued, or the work was stopped. The entire system could still issue, update and revoke identity certificates in a normal and safe way. At

```
root@coco-Vritualbox:~# openssl rsa -in rsa_private_key.pem -pubout -out
rsa_public_key.pem
Writing RSA key
root@coco-Vritualbox:~# more rsa_public_key.pem
------BEGIN PUBLIC KEY------
Jfaifofazuiofhqwiof Hfjiwfjia U83rjaoif94ioaj9q
fowfu4ifaH&U)UUOOUjoij8908t65nUOIJHIio
Aljiafjifjf824r943090
------END PUBLIC KEY------
```

Figure 5: Public key for certificate application

Table 1: Inquiry results of two public keys

Operations	Inquiry result of Node 1	Inquiry result of Node 2	Inquiry result Node 3
Apply correct public key to inquire	Certification passed	Certification passed	Certification passed
Apply random public key to inquire	Certification failed	Certification failed	Certification failed

the same time, the number of fault-tolerant nodes in the process of restoring the stopped nodes in the experiment process did not change. The reason was that the recovery of the nodes was equivalent to the consensus mechanism of the newly joined nodes participating in the competition for "billing rights". This process was equivalent to automatic synchronization data, which was a feature of the block chain that maintained usability.

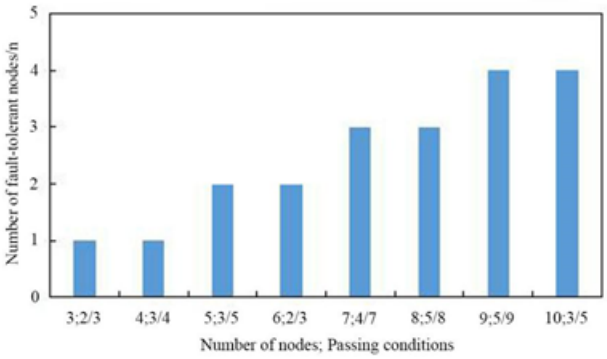

Figure 6: Number of fault-tolerant nodes under different nodes and passing conditions

The passing condition of the block chain was that the passing nodes was generally larger than half of all the nodes. At the same time, if the hacker wanted to destroy, steal or tamper with the digital certificate in the block chain, more than half of the nodes in the chain were needed to crack and attack since the nodes in the block chain were the same in the authority status. The encryption algorithm of the single node of the system required multiple computers to solve and the extremely long time simultaneously. As the nodes in the block chain increased, the fault-tolerant nodes also increased, and the nodes that needed to be cracked also increased, resulting in that it was almost impossible to solve more than half of all the nodes in the block chain at the same time in the actual implementation. Thus, block chain-based identity security authentication systems were extremely secure.

5 Conclusion

This study briefly introduced the block chain and the block chain-based identity security authentication system and simulated and analyzed the block chain and security of the system. By setting different test scenarios of the block chain, the block time and TPS were generated to measure the performance of the block chain. The security of the system were analyzed by stopping and restoring the node work to simulate hacker attacks. The results are that after the block chain issues a valid certificate according to the public key, it can accurately authenticate the user identity information of the input public key and prevent the non-authenticated identity information user from viewing the digital certificate. With the increase of nodes in the block chain, the passing conditions are continuously adjusted under the premise of guaranteeing that the passing nodes are more than half of all the nodes, and the fault-tolerant nodes are increased. The restored nodes can participate in the consensus mechanism normally. The difficulty of hacking attacks on tampering certificates is increasing. Security increases dramatically as nodes increase.

References

[1] M. Benchoufi, R. Porcher, P. Ravaud, "Blockchain protocols in clinical trials: Transparency and traceability of consent," *F1000Research*, vol. 6, no. 66, 2017. (doi:10.12688/f1000research.10531.5)

[2] C. H. Lee and K. Kim, "Implementation of IoT system using block chain with authentication and data protection," in *International Conference on Information Networking*, pp. 936-940, 2018.

[3] M. Fukumitsu, S. Hasegawa, J. Iwazaki, M. Sakai and D. Takahashi, "A Proposal of a secure P2P-type storage scheme by using the secret sharing and the blockchain," in *IEEE 31st International Conference on Advanced Information Networking & Applications*, pp. 803-810, 2017.

[4] X. Huang, C. Xu, P. Wang, *et al.*, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[5] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, *et al.*, "Quantum-secured blockchain," *Quantum Science and Technology*, vol. 3, no. 3, pp. 035004, 2018.

[6] H. W. Kim, Y. S. Jeong, "Secure Authentication-Management human-centric Scheme for trusting personal resource information on mobile cloud computing with blockchain," *Human-centric Computing and Information Sciences*, vol. 8, no. 1, pp. 1-13, 2018.

[7] J. H. Lee, "BIDaaS: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2018.

[8] C. Lin, D. He, X. Huang, *et al.*, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *Journal of Network and Computer Applications*, vol. 116, pp. 42–52, 2018.

[9] Q. Lin, H. Yan, Z. Huang, *et al.*, "An ID-based linearly homomorphic signature scheme and its application in blockchain," *IEEE Access*, vol. 6, pp. 20632–20640, 2018.

[10] L. N. Lundbaek, A. C. D'Iddio, M. Huth, "Optimizing governed blockchains for financial process authentications," *Cryptography and Security*, 2016. arXiv:1612.00407.

[11] T. Salman, M. Zolanvari, A. Erbad, R. Jain and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 858-880, 2018.

[12] H. Wang, Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 152, 2018.

[13] W. Yin, Q. Wen, W. Li, *et al.*, "An anti-quantum transaction authentication approach in blockchain," *IEEE Access*, vol. 6, pp. 5393–5401, 2018.

[14] R. Yu, J. Wang, T. Xu, *et al.*, "Authentication with block-chain algorithm and text encryption protocol in calculation of social network," *IEEE Access*, vol. 5, pp. 24944–24951, 2017.

[15] G. Zhitao, S. Guanlin, Z. Xiaosong, *et al.*, "Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities," *IEEE Communications Magazine*, vol. 56, no. 7, pp. 82–88, 2018.

Biography

Pengfei Fan, born in 1988-9-28, male, from Baotou, Inner Mongolia, China, has gained the master's degree. He is now working in State Grid Inner Mongolia Eastern Electric Power Co., Ltd. He is Network Security Engineer. He is interested network security.

Yazhen Liu, born in 1991-9-5, female, from Wuhai, Inner Mongolia, China, has gained the master's degree. She is now working in State Grid Inner Mongolia Eastern Electric Power Co., Ltd. She is Network Engineer. She is interested information communication network.

Jiyang Zhu, born in 1981-12-9, male, from Huludao, Liaoning Province, China, has reeceived an undergraduate degree. He is now working in State Grid Inner Mongolia Eastern Electric Power Co., Ltd. Information and Communication Branch. He is deputy director of Information Communication Operation and Maintenance Center. He is interested information communication networkand integrated management.

Xiongfei Fan, born in 1984-4-29, male, from Baotou, Inner Mongolia, China, has gained the master's degree. He is now working in training center of Inner Mongolia Electric Power (Group) Co., Ltd. He is a trainer by profession. He is interested dispatching automation.

Liping Wen, born in 1991-09-05, female, from Hohhot, Inner Mongolia, China, has gained the master's degree. She is now working in Inner Mongolia Electric Power (Group) Co., Ltd. Hohhot Power Supply Bureau. Her occupation is to monitor and inquire about electricity. She is interested Business Development.