2018 the 3rd IEEE International Conference on Cloud Computing and Big Data Analysis

Research on Information Security Technology Based on Blockchain

Liang Liu
Shandong Normal University
Jinan, China
e-mail: liuliang@sdnu.edu.cn

Budong Xu
Shandong Normal University
Jinan, China
e-mail: norest@163.com

Abstract—**Information security is the key to the development of modern Internet technology. The distributed mechanism, decentralized mechanism, password mechanism and scripted mechanism of the Blockchain present a completely new perspective for the development of Internet information security technology. The Blockchain technology redefines the storage and dissemination methods of the information in the network. Neither participant needs to know each other, and nor does it require third-party certification bodies to participate. It records, transmits and stores transferring activities of the information value by distributed technology, ensures that data is not tampered and forged based on an asymmetric cryptographic algorithm, enables all participants reached a consensus on the status of blockchain data information. And from the current industry research on blockchain technology, it expounds the application of blockchain technology in identity authentication, data protection and network security. The Blockchain technology will be a great driving force in the process of information security technology change, and will have a far-reaching impact on the expansion of information security.**

Keywords-blockchain; distributed; timestamp; decentralized; information security

I. INTRODUCTION

Information security involves all aspects of social life and runs through the entire process of national informatization. It is the focus of the national informatization construction and has a bearing on the practical interests of the vast majority of the people. In recent years, the social problems caused by information security have caused serious concerns from related departments, and more attention has been paid to security technologies such as system security, network security and data security involved in information construction.

Blockchain technology is the foundation for the construction of Bitcoin data structure and transaction information encrypted transmission [1]. It not only provides support for the operation and development of bitcoin, but it is also driving a revolution in information security technology. Blockchain technology will play a major role in identification and certification, defensing against DDos attacks, ensuring data integrity and credibility, and can actively promote the healthy development of national information security.

II. BLOCKCHAIN TECHNOLOGY

A. The Concept of Blockchain

Blockchain technology comes from a classic mathematical problem: the Byzantine failures, a fundamental issue in peer-to-peer communications proposed by Lesley Lambert [2]. The essence of the Byzantine question is that it is impossible to try to achieve consistency by means of messaging on the unreliable channel of lost information. Therefore, the study of consistency is generally based on the assumption that the channel is reliable, or there is no such problem. Under the Internet environment, when information value exchange with strangers is needed and the central node and routing can not guarantee complete trust, how can nodes on the network reach a consensus to prevent malicious fraud so as not to make wrong decisions? Blockchain technology provides a method to achieve without relying on a single node to create a network of consistency, so as to solve the Byzantine generals problem has long been known.

Blockchain technology, also known as distributed ledger technology, is an underlying technology that supports bitcoin operations, first appearing in Satoshi Nakamoto's essay "Bitcoin: A Peer-to- Peer Electronic Cash System " which is published in the Bitcoin Forum [3]. Blockchain technology is not a single and new technology, but a result of the integration of multiple existing technologies. These technologies are ingeniously combined with a database to jointly maintain a unique and reliable Database through a decentralized and trustful approach, and form a new way of data recording, delivery, storage and presentation. It is an Internet distributed database technology. The storage of traditional data information is usually done through a centralized data center. The difference between blockchain technologies is that anyone in the system can participate in the work of a data center. Blockchain technology removes the central control node by decentralized approach and constructs a P2P self-organizing peer-to-peer network by distributed method. Then, the blockchain technology maintains the integrity, continuity and consistency of data information through asymmetric password verification mechanism.

B. The Essence of Blockchain Technology

The essence of the blockchain is an evolutionary and scalable Internet protocol. Block-based chain data structure, open source decentralized distributed architecture,

978-1-5386-4301-3/18/$31.00 ©2018 IEEE

asymmetric cryptographic mechanism, flexible and controllable scripting constitute the core of the blockchain.

Blockchain technology is also an Internet distributed database technology, which is completely different from the traditional database structure. Blockchain technology uses Innovative block as a data element, the block through the index information connected into a chain, that is the blockchain. Data information is permanently stored in the form of a data record, and the file that stores data information is called a block. The first block is a genesis block, created by Nakamoto, and each block then chronologically records the value exchange during its creation, joining together to form a record set. Block structure contains the block header and block data, the block header links the previous block, and to ensure the integrity and consistency of the entire blockchain database, block data in the data record is validated value exchange information. Genesis block and block structure shown in Figure 1.

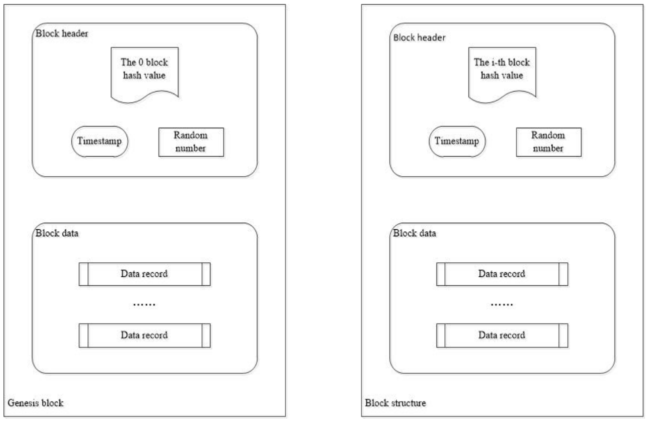

Figure 1. Genesis block and block structure

Therefore, the block structure has two characteristics: first, the data information in the block is all value exchange activity records during the time period from the creation of the previous block to the creation of the block, so as to ensure data integrity of the block chain database. Second, when the new block is created and linked to the end of the block chain, the block data of the block is complete, which ensures the consistency of the block chain database.

Block as a node based on the value of the exchange agreement to form a block chain, blockchain is the database shared by all nodes involved in the maintenance. Each block header contains the transaction information index of the previous block, so that the block is chained to the current block from the genesis block. If you do not know the index of the previous block, you can not generate the current block, so each block must be chronologically linked to the previous block. Therefore, the data index of the previous block forms the head of the block, the data information forms the block data, and the time stamp is affixed, then, formed a block chain end to end [4]. Blockchain data structure shown in Figure 2.

The magic of blockchain data structure: a block (complete history) + chain (full authentication) = a timestamp, which is the maximum innovation of the blockchain technology [5]. The blockchain database stores the complete data information from the genesis block to the latest block in a chain structure, and each data message can be traceable to validate its validity. The blockchain database allows anyone to participate in the recording of any block by a timestamp, which marks the authenticity of the blockchain database.

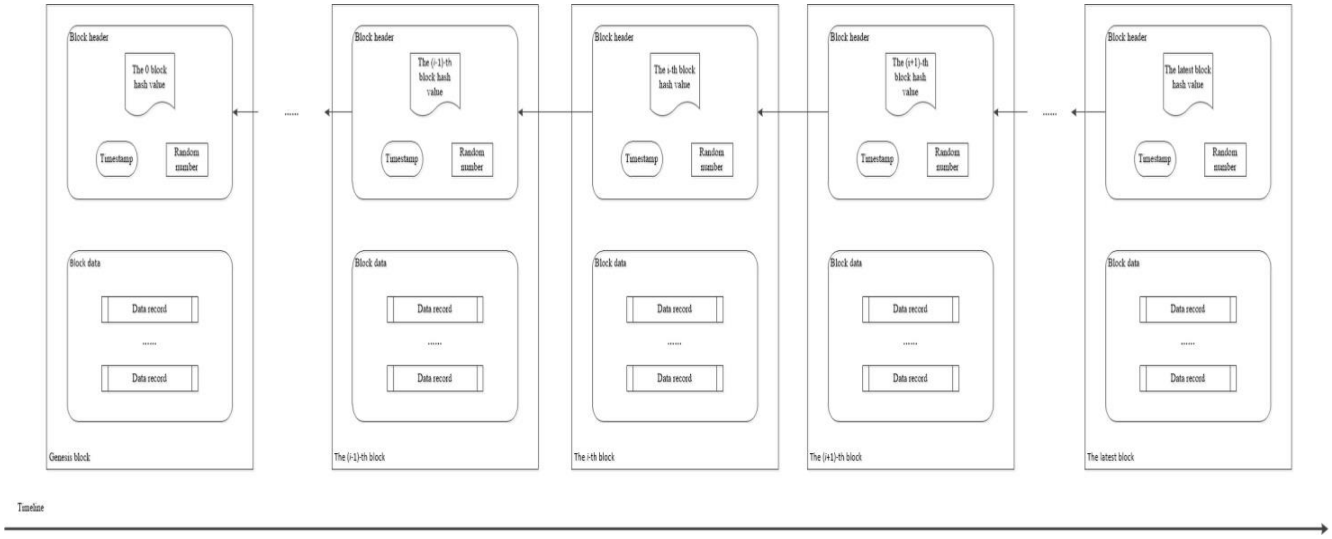

Figure 2. Blockchain data structure

Unlike traditional centralized data architectures, blockchain technology does not favor recording and storing data in a centralized data center for the recording and storage of data. Instead, all nodes work together to maintain all data. First of all, the blockchain constructs a set of protocol mechanisms. Each node of a peer-to-peer network has two tasks. One is to maintain the data information of its own node and the other is to verify other nodes. The updating of block data information relies on the fact that most nodes or all nodes in the network also consider the data information correct or all the nodes participating in the record pass the comparison result and the authenticity of the record is approved. Blockchain by building a distributed network system, all data are real-time updated and stored in all network nodes participating in the recording. Even if some nodes are damaged or hacked, it will not affect the data recorded throughout the block chain databases and information Updated. The distributed network system is based on the principle of voluntariness and establishes a distributed peer-to-peer network accounting system in which all employees can participate in order to decentralize accounting responsibilities. Then, data information is disseminated and validated in distributed networks via an open source and decentralized distributed system, stamped with timestamps to generate block data and disseminated and stored in a distributed network system. In the blockchain, new transaction information is also distributed in a distributed structure. According to the P2P network layer protocol, messages are sent from a single node to all other nodes in the entire network directly. Fully decentralized architecture real-time update data records in each network node to ensure blockchain database security.

The distributed accounting, dissemination and storage of blockchain technology shows that no organization can control the system. The processes of data storage, information transmission and transaction verification in the system are all decentralized. In other words, blockchain technology has built the first truly decentralized system in human history.

Blockchain technology validates the ownership of data information based on asymmetric encryption algorithms. Two keys are required for "encryption" and "decryption": a publickey and a privatekey. The publickey used to encrypt the blockchain is open to the public on the whole network. Everyone can use their own publickey to encrypt the information to ensure the authenticity of the data. The privatekey is only owned by the owner of the information. Encrypted information Only those who have the corresponding private key can decrypt, to ensure the security of data and information. Common asymmetric encryption algorithms include RSA, Elgamal, D-H, ECC, and so on. In blockchain system transactions, the publickey encrypts the transaction information, the privatekey decrypts the transaction information, and the privatekey holder decrypts it to use the value of the data it receives. The privatekey signs the data message, the publickey verifies the signature, and the verified message is sent by the privatekey holder. In the block chain technology, the two parties without know each other do not need to authenticate through a centralized certification body, just trust the algorithm-based trading rules to establish mutual trust and reach consensus.

In a decentralized environment, the script is a programmable smart contract that all agreements of the blockchain need to agree ahead of time. Blockchain technology uses a script to deal with sudden transaction patterns in the system and assures the practicability, flexibility and adaptability of blockchain technology in future applications. Scripts are essentially executable files based on a certain format. It is also a list of instructions that document the conditions for the value holder to obtain or spend on each value exchange activity. The programmability of the script is the flexibility to change the conditions under which the value of the saved-value is spent, as well as add some value re-transfer conditions when sending the value.

III. Exploration of Blockchain Technology in the Field of Information Security

A. *Identity Authentication*

Authentication is the process by which a computer system examines a user's identity, provides a mechanism for discerning and confirming user's identity, and determines whether or not the user has access to and authorization for system resources [6]. Its essence is to confirm the identity of the user, to protect normal legitimate users.

Authentication technology is the basis of security mechanisms such as access control, intrusion detection and security audit, and is the key of network information security. The current authentication technology mainly includes password-based authentication technology, PKI-based authentication technology, smart card-based authentication technology and biological characteristics based authentication technology [7]. The traditional authentication technology adopts the centralized authentication method. The CA (certificate authority) acts as the core of the authentication technology, realizing the functions of issuing, updating, revoking and verifying certificates. At present, most web application systems such as email system, messaging application system and portal website are based on the CA mode, are issued, activated and stored by the CA which is a centralized trusted third-party certification body to provide users with authentication services. There is a fatal security risk in this way, illegal users or hackers can attack CA center and fake user identity or crack encrypted information. Then, the system is cheated by getting the user's normal identity. Recently, WhatsApp broke the key re-negotiation mechanism loopholes that can be used by illegal users and hackers to send fake secret keys and the implement man-in-the-middle attacks to obtain data.

The identity authentication Based on blockchain technology has the characteristics of decentralized authentication and does not exist potential threats to central institutions such as CA. Moreover, releasing the key on the blockchain can prevent the spread of the fake secret key, and the application system can also identify the true identity of the other party in communication. Currently, the CertCoin project from MIT is the first PKI implementation based on blockchain technology. The CertCoin removes the centralized CA and replaces them with distributed accounts using blockchain as a domain name and a public key. In addition, after years of research, Pomcor has released a PKI implementation based on blockchain technology. In this way, you can keep the CA, but use the blockchain to store the hash value of the CA that have been issued and activated.

This approach allows users to authenticate the certificate through decentralized and transparent user sources, while improving network access performance by locally authenticating keys and signatures based on blockchain copies. There is also a noteworthy identity protection technology project IOTA. The project leverages Tangle, a lightweight, scalable and blockless distributed account, as the backbone for millions of IoT (Internet of Things) device interactions and point-to-point authentication with each other, without relying on third-party CAs, the project will be able to rebuild a completely new identity management system where no one can fake your identity by associating a personally identifiable hash table with a blockchain distributed account.

B. *Protect the Infrastructure*

The DDoS (Distributed Denial of Service) attacks combine multiple computers as attack platforms with the help of C/S (Client / Server) technology, launch DDoS attacks against one or more targets, so as to double the power of denial of service attacks [8]. The DoS (Denial of Service) targets exactly the "availability" of the three elements of information security - "confidentiality", "integrity" and "usability." The attack mode utilizes the defect of the target system network service function or directly consumes its system resource, so that the target system can not provide the normal service to the user.

There are many ways to DDoS attacks, the most basic DoS attacks take up too much service resources by using reasonable service requests, so that legitimate users can not get the service response [9]. When the attack target CPU, memory, bandwidth and other indicators of performance is not high, a single DoS attack on a one-to-one basis, the effect is very significant. With the development of computer and network technology, the destructiveness of DoS attack decreases due to the rapid growth of computational processing power of computers, increased memory, and increased network bandwidth. However, the Distributed Denial of Service (DDoS) attacks attack the victims on a larger scale by using more puppets (broilers).

The DNS (Domain Name System) service is the primary target for hackers to exploit DDoS large-scale attacks. In 2016, several records of the DDoS attacks announced that DDoS has entered the TB era. The use of block chain technology is expected to fundamentally solve the "Achilles' Heel" of the Internet, the DNS. Currently, the biggest weakness of DNS is caching, which makes DDoS attacks possible. It is also the cousin of the relevant departments to examine social networks and manipulate DNS registrations. Blockchain-based DNS systems register and resolve domain names using Ethereum blockchain and the IPFS (InterPlanetary File System) which aims to replace HTTP and build a better web for all of us. Its distributed storage technology will not only lose the focus of hacker attacks, but also a highly transparent, distributed DNS system can effectively eliminate any entity, including the arbitrary manipulation of records.

IV. Data Security

Data builds the foundation of the application system, and its integrity is the key to the data's value and the goal of data security technology protection. According to the method of cryptography, digital signature generates a set of data information representing the identity and data integrity of the signer, usually appended to the data file [10]. The user confirms the digital signature through the signer's publickey to verify the authenticity and integrity of the data information.

In general, the purpose of using a privatekey-based digital signature technique is for recipients or users to verify the origin of the data information. There is a problem here that the privatekey used for the digital signature needs to be verified that it has not been tampered with. But this contradicts the confidential nature of the privatekey, so digital signatures can only be used on the condition that the private key has not been tampered with. With the development of blockchain technology, the use of blockchain technology to replace the digital signature of data information can replace the secret with transparency, so as to distribute the evidence to a large number of blockchain nodes and increase the cost of tampering with the data. Therefore, it becomes almost impossible to change the data without being found.

GuardTime's blockchain technology-based KSI (Keyless Signature Infrastructure) project, a data security start-up company, is designed to replace the key-based digital signature technology. KSI stores hash tables of raw data and files on the blockchain, validates other copies by running a hashing algorithm, and then compares the data stored in the blockchain, any tampering with the data will be quickly discovered, because the original hash Tables are stored on millions of nodes. Matthew Johnson, the CTO at GuardTime, notes that KSI provides assurance of the whereabouts and integrity of data and information for the protection of sensitive data. Blockchain technology plays a significant role in securing data transparency, change escalation, and fine-grained accessibility of data information, which is significant for data operating organizations that deal with large amounts of sensitive data and suffer from frequent hacker attacks.

V. Summary

Blockchain technology explains a new way of trading based on key technologies such as password security, decentralized coherence, shared public accounts and visibility of its proper controls and permissions. It can completely change the way our society produces and lives by registering and exchanging assets which are physical and virtual, tangible and intangible.

Blockchain technology is not just an application technology for new-generation transactions. It creates trust, responsibility and transparency while simplifying business processes. It will completely change the way Internet transactions and bring about changes to Internet information security technology. The realization and application of any technology will inevitably face some security risks in the development process. However, the unique information storage and sharing method of blockchain technology is expected to bring a revolutionary solution to the unmanaged information security industry.

ACKNOWLEDGMENT

Supported by National Natural Science Foundation of China (61401260).

REFERENCES

[1] Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. Acta Automatica Sinica, J. 2016, 42(4): 481−494.

[2] MEI Haitao, LIU Jie. Industry present situation, existing problems and strategy suggestion of blockchain, J. Telecommunications Science. 2016, 32(11):134-138.

[3] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, J. Consulted, 2008.

[4] Melanie Swan, Xiao Feng. Blockchain: New Economy Blueprint and Guide, M. NEW STAR PRESS. 2016: 1-4.

[5] Lin Xiaochi, Hu Yeqianwen. A summary of blockchain technology, J. Financial Market Research. 2016(2):97-109.

[6] Liang Liu. Information security technology research in B2B e-commerce application system, D. North China University of Technology. 2013.

[7] Kong Gongsheng. Advances on secure authentication and trusted admission protocols for cloud computing, J. Journal of Henan University, 2017.

[8] ZHANG Yi-fan, DONG Xiao-ju. Visualization analysis and design of DDoS attack, J. Chinese Journal of Network and Information Security. 2017, 3(2):53-65.

[9] LI Yang, XIN Yonghui, HAN Yanni, LI Weiyuan, Xu Zhen. A survey of DoS attack in content centric networking, J. Journal of Cyber Security. 2017, 2(1):91-108.

[10] Lu Rongbo. Analysis and design of proxy signatures and group signatures, D. Southwest Jiaotong University. 2006.