ISSN: 2664-9640

Research on Computer Network Security Management Strategy Based on Blockchain Technology

Wei Jun [1,*], Xiaowei Su [2]

[1]Department of information engineering, Karamay vocational and technical college, Karamay 834000, Xinjiang, China

[2]Department of information engineering, Karamay vocational and technical college, Karamay 834000, Xinjiang, China

Abstract

With the update of computer technology, in the current era of big data, the continuous development of the Internet, cloud data, artificial intelligence and blockchain, network security issues are also gradually updated, and have received unprecedented challenges.The continuous generation, increase and saturation of data will inevitably lead to data security problems. Therefore, it is necessary to formulate relevant strategies for potential security risks to better guarantee the security of the Internet, protect the property and personal privacy of netizens from infringement, and make contributions to national network security.At present, the main risk types of network information security mainly include virus transmission risk, vulnerability attack risk, information invasion risk and hacker risk.Because blockchain technology has the characteristics of decentralization, tamper-proof, traceability, detrust and smart contracts, it has technical advantages in network information security applications.Blockchain technology can enhance the storage and sharing capacity of network data, improve the confidentiality and the integrity of network data, ensure the security of users 'private information, and conduct intelligent security management of assets and network transactions, so as to comprehensively protect the security of users' network use from multiple angles.

Keywords

Network information security; computer network; blockchain technology; encryption technology; security management.

1. Foreword

Network information security includes not only the security of structural system, but also the operation security and software application security, network information security system is fragile. If the lack of effective protection, it is easy to steal information by others and even affect the security of funds.Some LAN subject security access level is set too low, some computer software programs are not perfect, network system vulnerabilities, are easy to bring opportunities to the virus transmission.At present, the main risk types of network information security are virus transmission risk, vulnerability attack risk, information invasion risk and hacker risk, so corresponding measures should be taken to deal with them[1].

With the continuous development of modern information technology, the application of blockchain technology in network information security is becoming increasingly extensive.Blockchain is actually a decentralized ledger distribution technology, which gives users the strongest security guarantee through multi-level encryption technology, and also facilitates the use of transactions, social networking and other network information on the network through the real-time recording of the system.Blockchain technology has improved

ISSN: 2664-9640

the protection ability of network information security, reduced the system vulnerabilities, and greatly improved the network information security environment.

2. The hidden danger of computer network security in the big data environment

2.1. Viral threat

Network virus is a very common network security hazard, since the popularization of the computer has been an important security problem, not only will threaten the working environment and life of computer users, but also will cause the computer itself hardware and software problems, and even cause the system collapse and can not be used.Network virus often exists in some Trojan software or malicious website, in the bad website link also has hidden.Nowadays, with the popularity of smart phones, the number and types of network viruses on mobile terminals are also increasing, seriously threatening network security, and due to the replication of viruses and its wide spread, it is easy to invade mobile phones and computers and cause major hidden dangers[2].

2.2. Network fraud

In the big data environment, due to various app reading data, it is easy to cause personal information to be used by criminals, thus greatly improving the frequency and success rate of network fraud[3].Criminals use the Internet as a cover to carry out a variety of hidden fraud, induction or information behavior, use people's sympathy, money and personal negligence to cheat, has a significant impact on people's property safety.

2.3. Hacking

In addition to fraud, many malicious hackers are also lurking in the Internet, or collect top secret information, or invade the system to destroy competitors, or malicious engaged in spy, spy work, will have a bad impact on China's Internet information security.Hackers will also steal trade secrets and steal personal information to sell to others, thus causing heavy losses to companies or individuals[4]. [5].

3. The analysis of the factors affecting the computer network security

3.1. Physical security

To maintain the network security, we must first maintain the physical security of the network environment.Physical security is mainly reflected in the security of transmission equipment, such as computer, network signal base station, LAN, which requires network engineering designers can be optimized on the basis of the overall performance of equipment, ensure mass equipment can run normally in a safe network environment, should also properly receive individual user request, according to the actual situation or free or paid to help individuals solve the security problem of network equipment.Physical security factors require the computer users to have a basic and comprehensive understanding of the computer, and prohibit the personnel without any computer experience and basic education to use the computer to upload and save important information.Operators should pay attention to fire prevention and moisture-proof when installing equipment in the machine room, but also pay attention to the possible interference of other equipment electromagnetic waves on the computer equipment, and do not let the computer work in excessive dust or too cold overheating environment[6] [7].

3.2. Information and content security

To maintain network security, information security is more important, because information is the main content of network transmission, and it is the core of the whole Internet carrier and

ISSN: 2664-9640

communication.At present, there are a lot of criminals through mining others 'information content through this channel to obtain other people's bank card password, or tamper with user information for profit, has caused a bad impact on computer users.Information content security factors need to be paid special attention to.

3.3. Data dissemination security

Due to the data transmission in the network needs and protocol, and the website certificate, protocol and operation method and various software programs are not perfect, have the possibility of vulnerabilities, which means that Internet users may due to probability or improper use of security problems in the process of data transmission, by others to obtain personal data, affect their work and life.In addition, there are special hackers and others to destroy the user's system, which will pose a threat to the whole network.

3.4. Management of security

Management factors in network security are also very important.Any field needs people to maintain order, and of course, the Internet is no exception. Management security mainly refers to the maintenance, prevention and problem solving of the public security organs and Internet security staff on the Internet operation.When there is a hacker attack computer system and virus Trojan spread, the relevant personnel timely management of the Internet, intercept virus and hacker operations, and within the conditions of the network security personnel sanctions, so as to better protect the security on the Internet, to give the public a harmonious Internet environment.

4. The technical advantages of blockchain in computer network security

4.1. Decentralization

In the new era, in order to improve the network information security management, the use of blockchain technology has been the trend of The Times.Block chain system using partition data management structure, and detailed contract mechanism, to complete the system node independent interaction, making the user without intermediary mechanism of data storage and maintenance, has the characteristics of decentralization, can effectively prevent accidents, system intrusion security factors caused by information loss, information and leakage.

4.2. Immutability

The data acquired and stored by blockchain users on relevant nodes is unique and needs to be authenticated by the system and opened with specific secret keys, so other users avoid tampering with the data.On the other hand, the block chain block has hash value, disruptive properties, if the user in the block chain information is modified by others, the system will be the relevant block hash overall change, resulting in the block after information completely invalid until restored to previous data, to ensure the block chain.

4.3. Traceability

Block technology time stamp technology, the computer system recorded information according to time and categories into chain structure, combined with the corresponding algorithm to ensure the data traceability, in the process of writing the data traceability node can view and save all information and transactions, to effectively ensure the network system data information traceability and integrity, and to find the purpose of the data and use the data, on the one hand, on the other hand in the data download, viewing and transmission process are not disturbed by external unsafe factors.

ISSN: 2664-9640

4.4. Detrust and smart contracts

Blockchain system has asymmetric system encryption technology. In the process of data interaction, there is no need to judge whether trust and the degree of trust. The data exchange between different nodes can not deliberately prevent the dependence on the trust degree of central endorsement.In addition, due to the particularity of its own code and decoding, blockchain technology has the characteristics of automation and intelligent security protection, which can intelligently execute and supervise the operation process and trigger rules, so as to effectively provide data support in the field of network information security.

5. The role of blockchain technology for network information security

5.1. Enhance the storage and sharing capacity of network data

Block chain technology based on consensus system and resource sharing system technology for network data storage for the first encryption and secondary encryption, each encryption can fully guarantee the Internet security and information storage, in the first encryption, block chain using the block network key, will only the user knows the secret key through the block conversion lock mode as a protective zone, avoid the computer firewall security and problems, this level is enough to deal with most of the information security problems.The second layer of encryption means is the real-time guarantee area generated by the blockchain using its decentralized features, where the important content of the guarantee area is set and compared and verified through the database. It is determined that the users themselves use it, which also improves the storage security of network data.In terms of network data sharing, blockchain technology uses the data node information sharing mechanism. On the one hand, it is convenient for the other party to quickly and effectively accept the key information conveyed by users, and on the other hand, it can also prevent the receiver from tampering with the user's original, because it is irreversible, so it will be more secure.

5.2. Improve confidentiality and network data integrity

Due to the special encryption technology of blockchain, the arbitrary reading of network information is effectively contained, and the confidentiality of network data is strengthened.On block chain, on the other hand, because the information is multi-node transmission, the data on the system must through the relevant code and secret key can play a role, coupled with the visibility of the block ledger, strengthen block chain timely mechanism in network data transmission, when abnormal intercept, the system will automatically close the block information display channel, to ensure the user's information security is not stolen.Merkle technology in blockchain technology can use a variety of methods to ensure that data is not missed, tampering and lost, and even in the case of insufficient storage space can start the reserve, to ensure the integrity of the data, on the other hand, blockchain mihash function through scientific and effective calculation and automatic distribution system function, to make data tree structure, complete and orderly distribution arrangement, arrange data can effectively display through the blockchain partition, greatly facilitate the user's security data operation.

5.3. Ensure the security of users' private information

Users through the block chain to social networking, software download and surfing the Internet, block chain will before the user login account using special encryption encryption, the user in the process of use without the conventional password input, but with hidden password, to reduce the login process information stolen or even threaten the user's property security.Under the protection of blockchain technology, the initial data of their accounts will be stored in the distributed ledger, and the ledger will automatically open a fully blocked firewall. Only after triple verification can complete information be displayed, so that personal privacy can be

ISSN: 2664-9640

guaranteed, and the security of private information is continuously strengthened.In addition, blockchain technology can make use of the correlation between nodes to realize the effective dissemination of information in a very short time, and block all other non-willing propagation channels, so that the network communication can operate stably and reliably.If any node suffers a network attack during communication and information transmission, the blockchain system can still continue to operate with decentralized characteristics, thus realizing the barrier-free transmission of information.

5.4. Can conduct intelligent security management of assets and network transactions

Because the blockchain technology has a time-stamp and tamper-proof characteristics, its application in the Internet asset management and transaction frequency is also very high, which can effectively guarantee the security of transactions.Blockchain technology can effectively record, authorize and confidential track users' assets, and open further asset management and transactions through the authorization and signature labeling of asset owners as guidelines.The use of blockchain technology in points, digital currency, intellectual property rights, financial investment and other fields can make asset flow more effective, avoid the double flower problem in the process of digital transaction, improve the convenience of users for asset management, and effectively guarantee the security of assets.Block chain technology can effectively trace any changes in assets, and use the block distribution for permanent records, and due to the particularity of the secret key, only the asset owner can see and operate, in the process of asset view and transaction, block chain system will repeatedly through various means to prompt the user ongoing asset related operations and capital changes, so as to strengthen the user's vigilance, promote network asset management and transaction more intelligent and security.

6. Computer network security management strategy based on blockchain technology

6.1. Strengthen the control of network access and data encryption

In the big data environment, to network security management, should strengthen the control of network access, to take advanced security measures, strict authentication and control the user access to network resources, access frequency, access motivation, and when necessary for real-time tracking monitoring, in order to better prevent users with illegal purpose access.Comprehensive authentication can be conducted by adding identity authentication, using password password, increasing verification code and verification text operation, setting text permissions and so on, so the result greatly reduces the risk of the network user.To strengthen the encryption of data, should be according to the importance of data and the top secret degree to take different levels of encryption measures, the integrated use of network data and block chain relationship and interaction, the network key as far as possible, and the comprehensive change of data storage carrier, set up fine encryption algorithm, to ensure that the data encryption measures are constantly improved.In the process of data encryption, attention should be paid to the hierarchical and type encryption according to the source and flow direction of the data, so as to optimize the resource allocation more targeted and better strengthen the security of network data information.

6.2. Strengthen the isolation of the network and the detection of the intrusion

Should use firewall technology to implement network isolation, in data storage system, and the network is divided into internal and external parts, and according to the access to stipulate who can access the network, who can access the network, to form a certain degree of differentiation, prevent plot easy to obtain important information and resources on the Internet.To strengthen

ISSN: 2664-9640

their own system immunity to prevent the penetration of illegal virus, should be for various invasion of data, users, traffic, files, intrusion detection, preset information timely collection, and the user's past records and suspicious operation behavior detection, suspicion, verification and final confirmation, let the user on the premise of avoiding abuse of resources better improve the security of the Internet, and can contribute to better screening network crime.We should take good measures for virus prevention and control, strengthen security audit, timely vulnerability repair and system update, so as to effectively block the virus from the operation track of the system itself.To download legitimate software, prevent the behavior of virus piracy software, shall take virus prevention first, complementary comprehensive measures, earnestly daily safety maintenance work, for the virus to timely kill and source, and sufficient isolation, to prevent more user system infection virus.Should strengthen the audit of network data security, through network bypass, and restore analysis packet, access the key information accurate records, unified setting rules, and optimize the operation mode and strategy, for the network of abnormal mirror recording and screening, and through the system alarm intercept, so as to protect more network business normal and orderly.

6.3. Make good data backup to improve security awareness

Backup data is one of the important methods to protect network data, but also the core method, not only can prevent data loss, but also can restore data in the case of data damaged by attacks, so that Internet users can use and transmit network data more safely.To do a good job of data backup, strengthen the adequacy and necessity of the backup system on each computer, optimize the backup environment, ensure that the network environment is not abnormal before data backup, and set up a password to prevent others from stealing data.We should constantly improve the safety awareness, comprehensively train the public safety prevention methods and awareness, publicize the role and function of data security, and help the public to attract attention and vigilance, so as to prevent problems in the bud.We should be committed to the establishment of a perfect network security management rules and regulations, and improve the evaluation system and mechanism, the major problems caused by network security related accountability, and publicize the excellent deeds of network protection for positive teaching materials education, so as to achieve the positive strengthening effect of network security protection.To cultivate users consciously install anti-virus software, timely update patch consciousness and attitude, should realize in the thought with the development of science and technology, network security may also face more cutting-edge technology virus invasion challenge, only set up the crisis consciousness, can in the network security problems in good state, should change[8].

7. Peroration

To sum up, block chain technology can provide safe and reliable technology for network information security protection, and through the powerful system to realize the combination of security and intelligent, let the user in the process of using the network from malicious attacks and property losses, and protect personal information and other privacy, in the information transmission at the same time to better strengthen the immunity of computer system.Therefore, better popularizing the blockchain technology in the application of network information security can make an indelible contribution to the comprehensive construction of the social security system.

Reference documentation

[1] Wu Zongwei. The application of Blockchain in Network Security [J]. Electronic Technology and Software Engineering, 2019 (2): 207-207.

ISSN: 2664-9640

[2] Wang Yifan. Blockchain-based network security patent analysis [J]. Digital Design, 2019,8 (12): 32-32.
[3] Ye Junhong. The Application of Blockchain in Network Security [J]. Modern Information Technology, 2018,2 (11): 144-146.
[4] Hu Zhen, Liu Boya. The application of Blockchain in Network Security [J]. Electronic Technology and Software Engineering, 2019 (24): 175-176.
[5] Zhou Zongping, Li Jun. Analysis of the application of blockchain in network security technology [J]. China Informatization, 2020 (7): 76-77.
[6] in Jiahua. Research and Design of network security inspection based on blockchain [J]. Network Security Technology and Applications, 2021 (4): 28-30.
[7], Chen Xin. Network security analysis in the Big Data Environment [J]. Digital Technology and Application, 2017 (4): 222-223.
[8] High Dream Circle. Network security technology in the big data Environment [J]. Information and communication, 2017 (1): 158-159.