Universe
Scientific Publishing

Research on Security and Protection Strategy of Computer Data Based on Blockchain

Lei Zhang, Jian Xu
Taishan University, Tai'an 271000, China.

Abstract: From the perspective of computer data security protection, this paper explores the application of block chain technology from three aspects: cryptography technology, secure communication technology, access restriction and technology, this paper analyzes the advantages of block chain technology in computer data security protection, in order to maximize the computer data security. In cryptography, algorithms such as symmetric encryption and public-key cryptography provide multiple guarantees for computer data security. The technology of access restriction includes object access restriction, security judgment and so on, which improves the effect of data security protection.

Keywords: Blockchain Technology; Secure Communication; Access Restriction Technology

Introduction

Recently, blockchain technology has developed rapidly, creating a new model for efficient data processing, significantly enhancing the efficiency of data sharing, and improving the effectiveness of computer and data protection, it has opened up a new environment for data security. Blockchain technology, the practical application of technology, can complete the data removal between the points, strengthen the past, period of data tracing, established a non-trust relationship trading system. Blockchain technology, in the design and operation of development, full use of cryptography, hierarchical storage and other information technology, so as to form a new data processing system.

1. Application advantage of block chain technology in Computer Data Security Protection

1.1 Center removal function

Blockchain technology will be the data center removal function as the basic data processing, link. During the operation of blockchain technology, there is no dependence on any center, and with the support of distributed system, data processing such as data integrity, storage, data serialization update, etc. can be carried out efficiently, in order to build a trust system with no central dependence. In this technology environment, the system can not interfere with the overall operation ability of the blockchain network when the external factors attack any node of the system. In the blockchain, technical support, we should strengthen the application of the trust tripartite main body, to distribute the running ability, complete the center to remove the program, to achieve the same function operation, with data processing, the clarity.

1.2 The public nature of data records

Blockchain technology can carry on the data processing to the whole network node, by more advanced, the data processing form, enhances the data record, the data dynamic replacement transparency. Blockchain technology provides distributed accounting function for computer operation subject, and strengthens the integrity

of data storage from the distributed perspective. When the program running in each link of the computer network is in the open state, the open items include the program running in the network, the rules of the network structure, and the access form of the network nodes, so as to form the trust and trust framework of the blockchain. In the whole block chain network framework, the data storage function of transaction acquisition provides the node data download function for the computer operator, and records the user operation information at the same time, guarantee the openness of the data statistics of the node.

1.3 Making data tamper less likely

During the actual operation, the blockchain technology has the function of removing the center, configuring the distributed storage unit, setting up the data storage node in any computer program, and forming the data storage node copy, this maintains the standardization of data types when the nodes agree to store data. Therefore, when the blockchain technology runs and the framework reaches a large scale, the number of nodes will increase correspondingly, and the nodes will be divided and distributed on a large scale, thus forming a linkage system for controlling the whole network behavior, to ensure that each node of the network data storage regulatory effect, reduce the possibility of data tampering, . On the basis of a certain number of node data types, block chain data can be updated efficiently. At the theoretical level, when at least half a number of nodes are controlled, the network nodes can be effectively unified, thus reducing the cost of data security expenditure.

1.4 Anonymous schemes

The block chain technology effectively solves the trust and trust relationship among nodes, and completes the data exchange and data transaction in the form of anonymity. In the process of data exchange between nodes, it is possible to enhance the transaction in the form of a fixed algorithm, both parties predict, calculate and predict the subject of the computer's address, in the case of transaction, both parties do not disclose their identities, complete the data transaction, reducing the trust to determine the link.

2. Application of data protection based on cryptography

2.1 Symmetric encryption algorithm

Symmetric encryption algorithm can decrypt the same key algorithm efficiently. The two sides of communication should set up a secret key exactly at the beginning of establishing communication relationship. During the communication, the transmission of the secret key is completed, the clear text data can be encrypted, measures are taken, the ciphertext information can be obtained after the encryption processing, the receiver uses the key to decrypt the ciphertext, in order to ensure the security of plaintext transmission. In the actual operation, the symmetric encryption algorithm has a small amount of computation, but also has a more efficient encryption and decryption capabilities, so that the symmetric encryption algorithm has been widely used in computer data security. When both parties of the transaction share a set of keys, the security of the data can be guaranteed in the algorithm itself and the system. At the same time, the secure storage and the secure transmission of the key decide the whole security effect of the communication data. Therefore, the Encryptor should adopt encryption algorithm to ensure the security of encryption and encryption program, and give full play to the function of symmetric encryption. In the key encryption algorithm, including DES, AES two algorithms.

2.2 Public-key cryptography

The public-key cryptography algorithm has an asymmetric property, and in use it contains two keys for encryption and decryption. One of the two keys is a public key, the other is a private key. The public-key cryptography algorithm is used as follows: the computer user party a obtains a set of keys, the privacy key is stored securely by party a itself, and the public key is open to the outside world; When Party B uses the public key, it can

adopt encryption measures to the data, and then transmit the ciphertext to Party A; party a uses the private key to carry out the ciphertext analysis in an orderly manner. In the whole communication program, the data security of the computer user is guaranteed, and the security of the key transmission is not involved.

2.3 Hash algorithm

Hasche algorithm as a key component of cryptography, data in each, class length, can use Hasche algorithm to complete data length conversion, to enhance the effectiveness of data output. Under most conditions, the output of all kinds of input data is different, and the input information is quite similar, the output is also different, and there is no regularity of data output. Hashing algorithm has a single direction of use, can be efficient input data processing, computer users can accurately obtain the output results, however, in the output data, can not get the source data. Based on the use of Hasche algorithm, during the actual communication, data transmission user, can effectively complete data transmission, guarantee, corresponding to the integrity of the HACHY output, facilitate the receiver to effectively complete data reception. When the data receiver gets the data for the second time, the data is hashed and processed, and the result can judge the possibility of data tampering.

3. Secure communication protocol

When SSL protocol carries on the Security Communication, takes the digital certificate as the starting point. At present, SSL protocol has been widely used in web browser and web server, aiming at ensuring the data security of computer and improving the data security of information interaction, this protocol is applied at the connection location between the user operation layer and the TCP layer. The data information of user operation and Operation Layer is based on computer data. When the data is exchanged in the transport layer, it is transferred to SSL layer. SSL protocol encrypts the data it receives. At the same time, the SSL header is added before the first part of the message, and then the data information of the SSL header is added back to the transport layer. The SSL protocol consists of three elements: a handshake, a record, and an alert.

When the user computer terminal connects with the server, the SSL Communication Protocol is introduced, and the handshake protocol is used to guarantee the secure and secure data exchange between the user terminal and the server. In the user operation layer before the completion of the data interaction, the user, authentication, thus forming a data security communication system, to ensure the security of computing, computer user communication data.

4. Access restriction techniques

4.1 Object access restrictions

Object Access restriction is the determination of access rights based on the judgment of subject. In general, the role of access authorization is the object owner. For example, the access rights to files, folders, and shared data on a computer belong to the data owner. Data ownership, who can access data authorization, data access rights recovery operations, in order to protect the computer data security.

4.2 Access restricted security judgment

During security judgment, access to the object can be accurately obtained. In general, data security attributes and permissions belong to the computer administrator. Other users do not have the ability to tamper with this access restriction when it sets more stringent data security rules. Therefore should maintain the data original security attribute, by this safeguard access restriction validity, promotes the computer data security protection, the effect.

5. Conclusion

To sum up, from the perspective of computer data security, to strengthen the application of blockchain technology, maximize the protection of data security, improve the efficiency of data use, data security processing to create a new environment. Therefore, on the basis of blockchain technology, the integration of various data security technologies is completed, with a view to improving the data used by computers in various industries, ensuring data security, meeting the needs of computer use in various industries, and maximizing the visibility of blockchain, the application value of the technology.

References

[1] Mondain. Research on data security sharing mechanism under blockchain background [J] . Enterprise Technology and development, 2021(10) : 52-54.

[2] Shan, C., Application of computer network security technology in Big Data System [J]. Network security technologies and applications, 2021(09) : 82-83.

[3] Zhang, L., Security analysis of computer data based on block chain technology [J]. Wireless Internet technology, 2021,18(12) : 101-102.

[4] Zhu, X.M., Wang Chongyu, Zhu Yukun, Zhang Haifeng, Chen Ruidong. Blockchain based distributed network survivable data transmission technology [J]. Radio communication technology, 2021,47(03) : 277-283.

[5] Sun, Z.Y., Research on security and protection strategy of computer data based on blockchain. Electronic design engineering, 2020,28(24) :29-32+37. DOI: 10.14022 J. ISSN1674-6236.2020.24.006.

[6] Feng, Z.B., Fang, L., Application prospect of blockchain technology to enhance Internet of things security. Telecommunications network technology, 2018(02) : 1-5.