HILL PUBLISHING

Advances in Computer and Communications, 2023, 4(2), 89-93
https://www.hillpublisher.com/journals/acc/
ISSN Online: 2767-2875

Research on Computer Data Security and Protection from the Perspective of Blockchain Technology Support

Bo Li, Shi Li*

Chongqing University of Technology, Chongqing, China.

How to cite this paper: Bo Li, Shi Li. (2023) Research on Computer Data Security and Protection from the Perspective of Blockchain Technology Support. *Advances in Computer and Communication*, 4(2), 89-93.
DOI: 10.26855/acc.2023.04.005

Received: April 15, 2023
Accepted: May 12, 2023
Published: June 9, 2023

***Corresponding author:** Shi Li, Chongqing University of Technology, Chongqing, China.

Abstract

In the network era, the amount of data has surged, and a lot of data information has high density and high value information attributes, which also makes the problem of data security protection arouse the continuous attention of the society. Based on the purpose of data protection, people began to discuss the data security protection measures from the perspective of blockchain technology support. It is hoped that the development and application of blockchain technology can reduce the risk of damage in the process of data information exchange, accelerate the sharing of information data, and realize the marginalized processing of information ontology value, so as to maximize the stability of information transmission and ensure information security. This work first discussed the problem of computer data security and protection from the perspective of blockchain technology support, then clarified the specific measures of security protection and the application value of blockchain technology in computer data security, and finally provided certain theoretical research support for computer data security and protection.

Keywords

Blockchain technology, Computer, Data security, Protection applications

1. Introduction

As an emerging technology, blockchain technology is in the stage of rapid development, which provides multiple supports for efficient data processing. It not only drives data sharing and transmission, but also improves the efficiency of data sharing, highlights the value of data, and realizes the effective protection and deep utilization of computer data [1]. Blockchain technology is called an "umbrella" for data utilization. Its protection principle is also relatively simple, which strengthens the removal of point-to-point data, deepens the traceability of previous data, and establishes a transaction system without trust relationship. Based on information technology such as cryptography and tiered storage, a new data processing system has been formed. In this way, symmetric encryption, asymmetric encryption and other algorithms provide multiple guarantees for computer data security, and the data security protection effect is better [2].

2. Blockchain Technology and Application Characteristics

As an emerging technology, blockchain technology has a broad application space and a bright application prospect. It is generally considered as a data storage carrier with distributed function, which is supported by all kinds of precision algorithms, consensus technology and transmission technology. In the process of the practical application of blockchain technology, it chooses the decentralized data processing mode, completes the underlying optimization

design, and timely extracts the value of the data block with the help of cryptography and various encryption technologies, to achieve the accurate measurement of various attributes of data information. To sum up, the blockchain technology has three major characteristics. First, blockchain technology can be traced back. This means that blockchain technology can track the whole process of valuable information or data in the network system, to realize the traceability processing of different data nodes. Second, blockchain technology is highly irreversible [3]. It takes the data transmission attributes as the core, reflecting the correlation attributes of data information and time points presented by different network nodes. It can also automatically lock the path of data transmission, so there is no risk of data coverage and modification, and it can improve the stability and security of data transmission. Third, blockchain technology is open. In the implementation process, blockchain technology is considered to be an automatic data transmission and integration based on the distributed framework. It can ensure the stable performance of the information ontology in the transmission process and guarantee that the structure and calculation meet the requirements of the paradigm, so that it can achieve the accurate elaboration of data value attributes. The open characteristics of blockchain technology can also effectively ensure that the receiver and sender of data transmission can clarify the evolution mode of data information synchronously, and enhance the security of data processing and transmission. Based on these characteristics, it is possible and necessary to strengthen the security protection of computer data with the support of blockchain technology.

3. The Performance of Computer Data Security and Protection from the Perspective of Blockchain Technology Support

3.1 Data decentration function

Data decentration function is a basic function of blockchain technology and plays an important role in basic data processing. During the use of blockchain technology, the distributed system can effectively carry out the batch data processing, including both data integrity storage and centralized data sequence update, to build a trust system without central dependence. The technical environment built by blockchain technology makes it impossible for external factors to attack system nodes so that the overall operation of the blockchain network is free from any interference. When using the blockchain technology decentration function, the application of the three parties should be strengthened to complete the center removal task with distributed operation capability, so as to improve the efficiency and accuracy of data processing [4].

3.2 Open data records

Blockchain technology has the function of data processing for nodes of the whole network. Advanced data processing mode can be selected to record and dynamically replace data. Blockchain technology can provide distributed ledger use support for computer operators. Distributed perspective makes data storage more complete. When the program of each link of the computer network is in an open state, the network operation program, network architecture rules, and network node access forms are combined to form a trusted blockchain trust framework. In the corresponding blockchain trust framework, the data storage function should be played to record the user operation information and ensure the comprehensive and accurate accuracy of all data statistics of the node.

3.3 Difficult information tampering

In addition to the data decentration function, blockchain technology can also set up a data storage node in any program of the computer with the help of its distributed storage unit mode. When each node reaches a consensus on storing data, the data type is standardized and maintained. Generally speaking, when the operation framework of blockchain technology is large, the number of nodes will increase accordingly, and the distribution of nodes will also form a larger scale. Thus it will constitute the whole network behavior control linkage system, guarantee the supervision effect of data storage at each node of the whole network, and greatly reduce the possibility of data tampering. Based on obtaining consensus on quantitative node data types, blockchain data can be efficiently updated in a short time. From the theoretical level, when the control of at least half of the nodes is completed with the support of blockchain technology, the effective unified control of the whole network nodes can be realized, reducing the possibility of information tampering and reducing the cost of data security.

3.4 Anonymous scheme

When blockchain technology operates in an orderly manner, it can also drive data exchange and promote data transactions in an anonymous form. When the data is exchanged between nodes, the two sides of the transaction can

be predicted by a fixed algorithm. The body of the prediction is the address of the computer. Data transactions can be completed even if the identities of the parties are not disclosed, which means fewer trust confirmations and a simpler process.

4. Construction of Computer Data Security and Protection Model Based on Blockchain Technology

4.1 Construction of a private communication network based on blockchain

The computer data security protection model based on blockchain technology is mainly composed of communication infrastructure equipment, upper-level communication network, and registration security center parts. Among them, the communication infrastructure is the basic work unit, and each independent communication infrastructure corresponds to a light node of the blockchain. The upper layer communication network is a software-defined decentralized network communication structure, including the blockchain network, satellite network, base station communication network composed of nodes elected in different regions. With the help of the upper communication network, effective communication between nodes of different geographical locations can be realized, forming a trusted communication network management center for certificate registration, certification and issuance. When the information is verified, it is finally connected to the blockchain network of each region. To sum up, the construction of the private communication network based on blockchain achieves the distributed node network authentication of the registration authentication model, establishes the corresponding authentication mechanism, builds the P2P distributed communication network, and then designs the anti-destruction multi-routing scheme, providing corresponding routing elements through the node routing storage and backup [5].

4.2 Design of survival target routing

In the specific application process of the private communication network, data exchange is often driven by cooperation between network nodes. In the same blockchain network, when the communication initiating node and the termination node carry out data transmission, the node needs to select the route through the algorithm and then carry out data transmission. However, considering that the network is affected by uncontrollable factors, it may be unable to form a link to affect the data transmission. Therefore, in some special scenarios of network data communication, after the execution of the live operation, it is necessary to select the trusted agent node between different small LANs efficiently, and reuse it in the authentication node. The agent routing network generates routing according to the ledger information owned by the node, which is less susceptible to external interference and makes the network communication more stable. At present, the main anti-loss routing scheme is to generate stable routes through ledger information and routing algorithm during node information exchange, and forward information through proxy nodes, so that network information can be transmitted more securely and stably.

4.3 Safe communication of network nodes

In terms of secure network node communication, the emphasis is on the effective construction of communication application scenarios. Conventional network node communication mainly includes communication private network, internal communication and cross-regional network communication. In the actual communication network, the characteristics of the blockchain decentration can be used to give full play to its advantages of point-to-point transmission, and optimize the design scheme of the dedicated communication network based on the blockchain. Networks are essentially hierarchical networks [6]. The first layer network is a software-defined decentralized network communication structure based on SDN, which includes the blockchain network, satellite network, base station communication and other networks composed of various nodes elected by different regions. The secondlayer network consists of multiple communication infrastructures and regional levels in different regions. The blockchain network is also known as the "small communication network".

5. Application Efficiency of Computer Data Security Model Based on Blockchain Technology

5.1 Destruction resistance

By using blockchain and making full use of consensus algorithm and ledger characteristics, the detection of viable nodes and the update of node information ledger are carried out within a certain time, so that the nodes in the network have more alternative schemes. It can avoid the failure or damage of communication nodes, and the network is still tentative broadcast problems. When force majeure causes the failure of some nodes in the network, the nodes can quickly build a path according to the existing information to ensure the network resistant transmission.

5.2 Anti-replay

The replay attack mainly occurs in the process of identity authentication. It sends the received packets to the target host to destroy the authentication correctness of the target machine. Therefore, when making the election record, the scheme is judged by adding time stamp and random number. The node only needs to save all random numbers in a short time, and the receiver determines whether the replay attack is attacked by verifying the time stamp and random number in the data packet. The advantage of using timestamp and random number in blockchain is that the data space occupied by random number is not high, and timestamp synchronization does not need to be accurate, which can greatly reduce the network overhead.

5.3 Traceability and non-repudiation

When the node enters the network, the public key generated and distributed by the registry can be identified, and only the node with a corresponding private key can carry out data operation. Therefore, in the communication, the node identity can be traced through the public key, so that the data packet has non-repudiation characteristics [7].

5.4 Anonymity

In data transmission, the scheme combined with the characteristics of agent can ensure the anonymity of the node transmission. The current node can only decrypt the address of the previous hop and the last hop, and cannot obtain the complete communication path of the source node and the destination node, so that the transmission between each node in the private communication network can be relatively hidden.

6. Research on Data Security Sharing Mechanism under the Background of Blockchain

6.1 Blockchain technology network data security sharing mechanism

According to the construction achievements of the current data security sharing platform, blockchain technology is considered to be the key technology to realize the regional division of the data nodes in the network and gradually detect the authenticity of the current data information. Based on the attribute analysis of regional network nodes, blockchain technology marks the entire data bearing area, enabling the data transmission type in the security area to be immediately detected, and supports the recording of time nodes of various data transmission modes. It can not only reduce the interference of external factors, reduce the risk of data transmission, but also reduce the cost of data information processing. The implementation process of blockchain technology can be considered to be the PKI trust value in the inherent data area, which is based on the service mode carried by the whole system as the entry point. With the authentication mechanism, identification mechanism and user system, the derivative effect of data in different regions in the reasonable access space is determined. With the help of the accurate docking of regional attributes, the data transmission based on the degree of trust is achieved. In this way, when the data information is confirmed, it will be independent of the entire transmission area, and the transmission attribute of the data information itself will be marked with a credit value. In the actual data transaction process, cross-domain authentication can be carried out from the user terminal and the receiving terminal, making the data information transmission more stable and secure, and preventing the risk vulnerabilities in the overall network architecture and data sharing platform.

6.2 Realize the security sharing of blockchain technology network data

From the technical point of view, when blockchain technology is applied in the whole network data security sharing platform, it adopts precision algorithm and combines the data structure to benchmark the block top-level design. In this process, in order to determine the security of all kinds of data and information transmission within the sharing framework, it is necessary to clarify the whole information subject, and then mark and authorize the data presented by the information nodes in different structures to ensure the request mechanism of the subsequent tasks in the operation process. From the perspective of data transmission, when users define various types of information, they start from their own demands and define the transmission paths of different uses or information through the attributes presented by the data information [8]. Blockchain technology realizes the authorization processing of relevant data through the instruction of the user, and ensures the transmission of the whole information within the network architecture in an identifiable and traceable mode to confirm the data. In this mode, data information can be stored and transmitted synchronously in the Intranet or the whole WAN. At the same time, the authentication function

of blockchain technology is to realize the regional construction of different network systems based on the distributed structure. Through the information sharing and transmission mode in the whole data security category, it can ensure that each kind of transmission structure and the network structure is supported by blockchain technology, forming the effective integration of a cloud server or computer network server.

7. Conclusions

By analyzing the characteristics of blockchain technology and its role in computer data security protection, it is not difficult to see that it is necessary to actively promote blockchain technology and give play to its value in computer data security protection. It is necessary to make great efforts in the research and development and application of blockchain technology, strengthen the integration of data security technologies based on blockchain technology, and enhance the security of computer data with the deep application of blockchain technology. Through multiple measures, a more secure data transmission and sharing application environment can be created, which can truly highlight the value of blockchain technology in information security protection, and also provide certain theoretical support for the promotion of the technology.

References

[1] Zeng, Z., Li, Y., Cao, Y., Zhao, Y., Zhong, J., Sidorov, D., & Zeng, X. (2020). Blockchain technology for information security of the energy internet: Fundamentals, features, strategy and application. Energies, 13(4), 881.

[2] Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, *7*(2), 189-208.

[3] Farouk, A., Alahmadi, A., Ghose, S., & Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. Computer Communications, 154, 223-235.

[4] Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications, 50, 102407.

[5] Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. J. C. C. (2019). Analysis of Blockchain technology: pros, cons and SWOT. Cluster Computing, 22, 14743-14757.

[6] Zhao, G., Liu, S., Lopez, C., Lu, H., Elgueta, S., Chen, H., & Boshkoska, B. M. (2019). Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions. Computers in industry, 109, 83-99.

[7] Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography, 3(1), 3.

[8] Khan, M. A., Abbas, S., Rehman, A., Saeed, Y., Zeb, A., Uddin, M. I., ... & Ali, A. (2020). A machine learning approach for blockchain-based smart home networks security. IEEE Network, 35(3), 223-229.