Access Control of Social Network based on Blockchain Technology

Liu Jianlan, Zhu Li, Xiong Guang, Li Yan, Xu Zhengze

Jiangxi Science and Technology Normal University, Nanchang, Jiangxi, 330038, China

Keywords: Blockchain Technology, Social Networking, Data Privacy Protection, Social Network Privacy

Abstract: Social network is the innovation of modern information communication mode. On the one hand, it is not only because social networks realize the perfect mapping of social relations in the virtual world in the real world.On the other hand, its good malleability and openness further expand point-to-peer to complex interpersonal networks. Users upload personal information on the platform, which includes public data and private data, and the data is stored on a centralized server. Users' data is used by the platform without their knowledge. Meanwhile, technical loopholes increase the risk of privacy leakage. When user privacy leaks are frequent, they bring considerable losses to users and platforms, and the attention to privacy has become more and more a problem that cannot be ignored today. Every year, about 80 million people's privacy is stolen.The development of blockchain technology has led people to consider applying new technologies to the privacy security of social networks. Technically asymmetric block encryption protects the confidentiality of user data; decentralized technologies will be used to establish decentralized database systems and consensus mechanisms to protect data integrity, a more secure storage method than traditional technologies. In social networks, the application of clustering technology focuses on data protection, data security storage, and authentication to meet the basic needs of user data protection and security. Data protection and security issues are becoming increasingly apparent, and the public begins to understand their privacy and security. The technologies used in blockchain can bring new changes to centralized social networks in traditional environments. The paper uses literature research, quantitative analysis and qualitative analysis methods to elaborate the basic theories of "blockchain" and "social network", and designs the private data processing scheme based on blockchain technology. The results show that blockchain has high performance characteristics in processing private data.

1. Introduction

Social networks map real-world social relationships on the Internet. Social network is an open network, and users need to broaden their interpersonal boundaries by uploading and displaying some personal data to social network service providers. If you have a large number of personal information, such as name, age, education, contact information, workplace, social friends, etc., automatically download [1]. User information includes public information and personal information. Once uploaded, they will exist on the platform for the long term but not in the short term, which increases the possibility of privacy leakage. At the same time, because the information transmission is point-to-point and divergent transmission on the social network, it increases the uncontrollability of the data.Various applications of different networks are increasingly common, bringing great convenience to the country, society and individuals, such as government affairs, management, finance, online shopping, social networking and other fields. Data mining technology continues to deepen, how to protect privacy while enjoying services is an urgent problem to be solved. Privacy issues cover almost every corner of the Internet, and have gradually become a huge stumbling block to the progress of the Internet technology, [2].

Scholars at home and abroad have always attached great importance to the protection of personal privacy information, so there are many research results in related aspects, and the fields are extremely diversified.In terms of the model research of privacy protection algorithms, in order to avoid leaking the privacy information during the data storage and use process, the relevant

  DOI: 10.25236/iwmecs.2022.006

researchers propose a series of related algorithms and model [3]. In general, there are mainly association rules and classification algorithms, while the clustering algorithms are relatively few. At the same time, on the basis of combining the classical statistical regression methods, the anonymous algorithm and clustering algorithm have been optimized and improved and successfully applied in the process of personal data privacy protection. In terms of key technologies of privacy protection research, in terms of data processing methods, the following privacy technologies are mainly used: privacy technology based on data encryption, privacy technology based on data distortion, and privacy technology due to limited disclosure. Data encryption technology mainly uses methods to hide sensitive information. Especially in decentralized cluster environments, it usually must implement data protection on the basis of ensuring communication security, and the encryption technology can match the requirements.Therefore, data encryption technology is often used in distributed environments, and its main algorithms include secure multi-party computing, distributed mining, distributed clustering and other [4].

The rapid development of technology not only brings convenience to people, but also generates serious privacy problems. If the privacy issues are not valued and solved, they will seriously restrict the innovation and development of technology. At present, privacy has become one of the huge obstacles to the further development of network technology. If privacy cannot be protected, all kinds of user data and related privacy may be stolen, which will seriously hinder the trust of individuals and enterprises in technology, and then hinder the progress of technology [5]. Therefore, privacy protection technology is particularly important. Predictably, block chain technology and distributed database in the future will greatly promote the reform of social network privacy of data, with to (weak) centralized, traceability and tamper-with typical characteristics and distributed data storage high computing power, large capacity storage, scalability, cost saving technology advantage, make the technology and application gradually began to the distributed environment, this naturally will bring some important problems.

2. Proposed Method

2.1 The concept of blockchain technology

With the development of blockchain technology, it is increasingly linked to the applications of various scenarios, which can be regarded as a product structure with open, transparent, traceable and unmodified data[6]. It gives data with new definitions of data deployment and storage by combining P2P network, encryption technology, data storage technology, and distributed algorithm. As an important data structure in the blockchain, the hash pointer is designed based on the hash algorithm. Unlike standard characters that can only describe the data store location, a hash pointer can not only describe the data store location, but also check if the data has changed. In terms of infrastructure, the department chain is mainly divided into six levels: application layer, contract layer, incentive layer, consensus layer, network layer and data layer. The data storage and encryption techniques behind the blockchain are embedded in the data layer. In the data layer, events must be encapsulated in data blocks associated to the chain structure. Different encryption functions are used to ensure data integrity and reliability. P2P technology has been implemented at the network level, its main purpose is to realize random topology between blockchain nodes and conduct effective distribution and local authentication of updated blockchain data; the consensus layer containing consensus algorithms used in different block networks is the key to maintaining the standard state of P2P blocks.

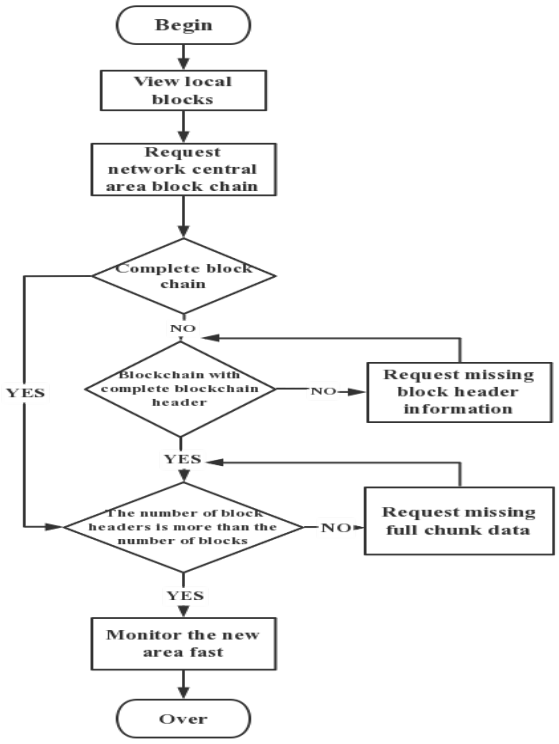

Figure 1. Map of the block-chain synchronization flow

2.2 Classification of blockchain

According to different service objectives, blockchain can be divided into public chain, private chain and alliance chain.Public network —— Public block network —— is a fully open block network. Anyone who does not need an ID can always log on to the system to receive information, send transactions, and validate transactions.A blockchain form of, in which everyone can compete for accounting rights[7]. The public chain is similar to a public ledger, everyone can freely enter and exit the blockchain network, and can have access to complete ledger information, and become a participant in the maintenance of the blockchain and accounting rights competition. The private chain is relatively closed relative to the public chain, which refers to the blockchain form whose writing authority is completely controlled by individuals or internal organizations, and whose data access permission is strictly controlled. Unlike the public chain, the private chain cannot strictly be called a blockchain. It is more like a private ledger of an enterprise or individual. Only users who meet specific conditions have the right to go in and out at will. An alliance chain is a blockchain between the public and private sector managed by multiple organizations or institutions. In the alliance chain, each organization or organization is responsible for the operation of one or more nodes, and only the organization or organization involved in the management has the right to receive, record and submit the alliance chain data and record the transaction data in that chain.

Table 1. Comparison between public, alliance, and private chains

Characteristic	Public chain	Alliance chain	Private chain
Trading party	All nodes	Alliance member nodes	Private node
Consensus	All nodes	The alliance selects nodes	Custom Node
Excitation mechanism	essential	Selectable	Selectable
Tamper with sex	Almost immutable	May be tampered with	May be tampered with
Productiveness	low	tall	tall

2.3 Social Network Definition

From the birth of the Internet Web2.0, and with the rapid development of intelligent terminals and mobile Internet, social network service has become one of the most popular services on the network, now social network has been a social relationship have offline to online mapping, it has the basic social functions, become an irreplaceable part of people's daily [8]. Social networking (social network) works to create an online community for a group of people with the same interests and activities. These services are often based on the Internet to provide users with various connections and communication channels, such as email, instant messaging and information distribution services, which have three abstract characteristics for individuals: (1) allowing users to build public or semi-public space in a bounded system; (2) allowing users to share information and other users; and (3) allowing free connections between users, which differ from the platform that provides network services.Social networks provide users with a variety of ways to interact with information, such as chat, sharing files and others[9].

2.4 Social network privacy

In the network personal privacy often appears in various forms, the first is personal basic information, including the mobile phone number, name, age, etc., the second is the personal network property information, such as bank account password, etc., the third is personal dynamic information, text information, video and photo information; the fourth is the user private interaction information, such as personal browser search history, personal Internet IP address and click history. Of course, according to the actual difference, not all personal information in situations should be regarded as privacy. It can be said that personal information is privacy in a certain situation, but may not be privacy in another situation.Nowadays, social networks can be said to be a high incidence area of user network privacy leakage, bringing the high sensitivity of users' privacy attention[10].

3. Experiments

3.1 Experimental Subjects

The paper mainly introduces the social network development in the Internet, at the same time social network user privacy data leakage caused the society and users for their social network platform data security attention, and block chain technology is used to solve the problem of social network data privacy security, as the background to the main research direction of this paper. By reading a large number of literature, expounds the "block chain", "block chain classification", "social network" and other basic theory, review the social network research situation, to further expounds the current privacy research, from the concept of network privacy in the field of social network, further analyzes the user privacy concerns and user privacy behavior, and then combed the block chain technology and theoretical research.

3.2 Experimental Methods

The paper mainly uses literature research method, qualitative analysis method and quantitative analysis method, through combing the literature, fully clarifies the research methods and research results related to social network, user privacy, blockchain theory and classification. Based on this, the applicability of relevant methods and theoretical models is further analyzed, and finally the most suitable research method is selected.Based on the private data, and the MapReduce computing framework is used to process the private data. The experimental results show that by comparing the experimental analysis with the original encryption algorithm, the model has a great improvement in computing efficiency, and has the advantages of high performance when the data amount is large.

4. Discussion

4.1 Effective processing scheme of private data based on blockchain

With the development of the Internet and cloud computing and the widespread use of blockchain technology, multi-party distributed computing has become the focus of attention. Reliable computing platforms based on blockchain take into account the problem of high computational complexity when processing big data. In order to improve the processing speed of private data on the blockchain, the consensus algorithm of PBFT is first appropriately improved to improve the consensus speed, and then the homomorphism encryption algorithm is appropriately improved. In order to improve the computing efficiency, MapReduce computing framework is adopted to achieve parallel processing.These aspects jointly ensure the effective processing of private data and improve the processing rate of private data to some extent.

4.2 Privacy data processing scheme based on MapReduce

Using homomorphic encryption algorithm to conduct privacy processing, data can protect the privacy of the data processor in the operation itself, can not view the personal details being processed, can only see the final result of processing.In conventional public-key cryptography, power functions or modular functions are usually used for encryption. While it provides security, the operation process is relatively complex. In this work, we propose a DGHV algorithm that can increase the range of homomorphism and coefficients. In previous systems, some encryption features required more space to store public keys, and the duration of encryption was inefficient, and some features led to simple data encryption.The encryption procedure uses the MapReduce framework to determine whether the master node is a node.In the case of mapping nodes, the improved homomorphic encryption algorithm encrypts the data obtained through parallel segmentation. If it is a restore node, the data obtained after combining the encrypted data is processed to obtain the output data.Finally, the encrypted message is placed in the chain, and the user manages the data with the public key. A user with the right to receive the correct information can only obtain the actual information with their consent.

The specific process consists of the following steps: (1) the participant enters the data to the client.(2) User submits operation function map ()reduce() to the client (3) blocks the data (4) The client submits operation function map () and reduce() to the Map Reduce system.(5) Job Client requests to a task through Job Tracker, does some check input work, then copies the resource call Submit Job() required for the request to the Job Tracker system and tells Job Tracker is ready to run.(6) Map end to partition the input data sorting operation (7) call the improved homomorphic encryption algorithm for encryption using the improved homomorphic encryption algorithm, Encrypting the results output from the map end in step 5, And store the encryption results into the local file system, And index (8) reducer copy each intermediate file output from the mapper side to the local file system, And merge the copied data files to (9) call the reduce( ) function for operations processing Reducer calls the reduce function provided by the operation provider, For the reduce processing of the file, Store the output results in the folder of HDFS (10) n participants to jointly decrypt to obtain the respective desired results.

In order to improve the efficiency of private data processing, in the present scheme, we first improve the consensus mechanism of PBFT, and the improved consensus algorithm improves the consensus speed between the blockchain nodes. The homomorphic encryption algorithm is improved, and M a p, Reduce computing framework is used for parallel processing of private data. The private data can be effectively processed through the above process.The following results were analyzed by experiments.In the experiment, the DGHV algorithm is improved to different degrees, and then the three algorithms can parallel encrypt the operation time with the number of Map nodes. In the experiment, the 128M file information was encrypted, and the improved algorithm was used to encrypt 8 bytes at a time, and the security parameter was set to 2.

Figure 2. The relationship diagram of the operation time of the three algorithms and the number of Map nodes

Two conclusions can be drawn from Figure 2. First, the running time of each algorithm decreases as the number of Map nodes increases. When the Map nodes increase to a certain value, the running time of the algorithm is usually stable. As the number of card nodes increases, the data is divided into multiple data blocks to participate in the operation, thus increasing the operation speed.Second, based on the DGHV algorithm, the least time is spent if the number of encrypted pure text bits is bits and the format of the public key component is used three times. This is because the number of digits or public key components increases, which shortens the length of encrypted text and thus reduces availability.

5. Conclusions

With the development of the Internet, especially the mobile Internet, social networks play a very important role in people's daily life.In recent years, active users and great creators have brought huge traffic and huge profits. However, the users who made the content did not have full control over their content or a full right to win.In addition, social media has serious security vulnerabilities, involving centralized storage of information and content, and may even leak users' privacy.Blockchain itself is characterized by distributed storage, dispersion, distrust, instability, and programmable. These functions enable the blockchain to make up for the shortage of the original centralized equipment, improve operational efficiency, reduce transaction costs, realize flexible changes in market rules, prevent information manipulation and manipulation, significantly improve system stability, and reduce the risk of default. Therefore, there are many application scenarios for blockchain, and many social networks are also studying the application of blockchain technology in the process of decentralized information storage and value transfer.There is an immeasurable future of using departmental chains on social networks to store content information and provide added value. This type of social network can bring more benefits to their users and return them to their users. Blockchain technology can solve some security problems in the centralized storage mode, making more and more social networks pay attention to user security, which is of great significance to the development of social networks.

References

[1] Zhang Y, Cui M, Zheng L, et al. Research on electronic medical record access control based on blockchain[J]. International Journal of Distributed Sensor Networks, 2019, 15(11):155014771988933.

[2] Zhang Y, Cui M, Zheng L, et al. Research on electronic medical record access control based on

blockchain[J]. International Journal of Distributed Sensor Networks, 2019, 15(11):155014771988933.

[3] Li X W, Chen Y, Zhu H Y . An Access Control Scheme Supporting Privacy Protection Based on Blockchain and Attribute[J]. Journal of Physics: Conference Series, 2021, 1966(1):012048 (14pp).

[4] Song L, X Ju, Zhu Z, et al. An access control model for the Internet of Things based on zero-knowledge token and blockchain[J]. EURASIP Journal on Wireless Communications and Networking, 2021, 2021(1):1-20.

[5] Bhushan B, Sinha P, Sagayam K M, et al. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions[J]. Computers & Electrical Engineering, 2020, 90(9):106897.

[6] Xu R, Yu C, Blasch E, et al. Exploration of blockchain-enabled decentralized capability-based access control strategy for space situation awareness[J]. Optical Engineering, 2019, 58(4):1.

[7] Shan S, Duan X, Zhang Y, et al. Research on Collaborative Governance of Smart Government Based on Blockchain Technology: An Evolutionary Approach[J]. Discrete Dynamics in Nature and Society, 2021, 2021(4):1-23.

[8] Qi Y, Wang X, Zhou Q, et al. Research of Energy Consumption Monitoring System Based on IoT and Blockchain Technology[J]. Journal of Physics: Conference Series, 2021, 1757(1):012154 (5pp).

[9] Li D, Yu J, Gao X, et al. Research on Multidomain Authentication of IoT Based on Cross-Chain Technology[J]. Security and Communication Networks, 2020, 2020(10):1-12.

[10] Tith D, Lee J S, H Suzuki, et al. Patient Consent Management by a Purpose-Based Consent Model for Electronic Health Record Based on Blockchain Technology[J]. Healthcare Informatics Research, 2020, 26(4):265.