Research on Multi-party Cooperative Secure Identity Authentication Mechanism Based on Blockchain

Nianzu Liu¹*, Bing Guo²

¹ College of Computer Science, Sichuan University, Chengdu, China, 610065
² College of Computer Science, Sichuan University, Chengdu, China, 610065
*Corresponding author e-mail: 2019223045144@stu.scu.edu.cn

Abstract. With the continuous development of information society, blockchain technology can play an extremely important role in many fields. However, with the increasing degree of communication in the information society, a huge amount of data is generated. How to protect the information data generated in the process of communication has become a more serious problem at present. In its earliest stages, blockchain technology was used only for cryptocurrency transactions. Under the general directory, there are a lot of sub-accounts, and these sub-accounts are all valuable accounts, and the data is stored in different blocks in different chains. Judging from the current application of blockchain technology, the application of this technology can guarantee the security of data storage. Data storage is extremely secure in terms of security, so there will be no individual or group to destroy or tamper with the data. In blockchain technology, all data is stored in a Mosaic form in many blocks, which means that a single block does not have the function of storing information data. When making a large transaction, due to the uniqueness of blockchain technology, each member of the chain needs to authorize the data, which means all members of the chain must agree to the transaction before the transaction can be completed. Starting from the application of blockchain technology, this paper analyzes the most common identity authentication mechanism in our daily life, and analyzes the application of blockchain technology in daily life from multiple aspects.

1. Introduction
With the continuous advancement of the information society, blockchain technology can play an extremely important role in many fields. However, with the increasing degree of communication in the information society, a huge amount of data is generated. How to protect the information data generated in the process of communication has become a more serious problem at present. The generation of blockchain technology can be up to this task to a large extent, and solve the problem of the huge volume of communication data caused by the upgrading of communication.

2. Knowledge of blockchain technology

2.1. Introduction to Blockchain
In its earliest stages, blockchain technology was used only for cryptocurrency transactions. Under the general directory, there are a lot of sub-accounts, and these sub-accounts are all valuable accounts, and the data is stored in different blocks in different chains. In this category of accounts, it is extremely difficult to create blocks because of the amount of computational effort and time required to create the...
blocks. Each block introduces part of the previous block, and in this way it continues, eventually forming a chain [2-3]. So if you want to create a piece of from it is extremely difficult, because every piece contains a portion of a piece of information, and the parts of the piece of information is also need to pass on to the next piece of storage, so want to tamper with the random piece of information is very difficult, if an individual or a company want to tamper with a particular piece of information, only to tamper with all of the block was able to achieve this goal, but it is not possible at the moment.

The chain is created using extremely complex technology, which makes the information stored in the block more secure and reliable. Secondly, blockchain technology does not have a central system to control all the data. The essence of blockchain technology is a database that can get rid of the total control system, and members only need to manage their own groups. No total control system means that no individual or group can tamper with or destroy the blockchain data unilaterally, which also makes the blockchain data more secure and reliable.

With traditional data storage, all data is stored in a single location that can be connected to the Internet or a portable hard drive. This creates a problem. No matter how carefully you store your data, there will always be traces of your storage that hackers can use to easily steal or tamper with your data. With the help of blockchain technology, data can exist in the form of blocks in the whole chain, and no individual or group can destroy or steal. The special structure and reliable parameters of the system make blockchain technology the most ideal choice for safe storage of data.

2.2. Advantages of blockchain technology
Judging from the current application of blockchain technology, the application of this technology can guarantee the security of data storage. [4] Data storage is extremely secure in terms of security, so there will be no individual or group to destroy or tamper with the data. In block chain, has a very important thing is that each member of the chain need to validate every item, in large part because line guarantee the authenticity of the data, data input to the all information in a block are unable to edit or delete, this means that each member of the chain to be able to see each entry, which could not be hiding information, realize the true sense of transparency. Since the technology has no substantial master control system, which means that no one or group has centralized authority to view the information in the block or control the transactions, this feature makes the application of blockchain technology in cryptocurrency more prominent. (figure 1)

![Figure 1. Advantages of blockchain technology](image)

2.3. Distributed storage of data
In blockchain technology, all data is stored in a Mosaic form in many blocks, which means that a single block does not have the function of storing information data. If someone wants to steal data information, so he didn't have a clear target to attack a block, only to attack the whole chain to obtain
want data information, but it is impossible in the block chain, let us, therefore, the application of the block chain technology data information become more safe.[5]Since everyone in the block has to grant every permission in the chain, and there is no way to edit or delete the data in the block, the information in the block is guaranteed to be true and valid. Since there is no central control system, there is no chance to operate on the whole chain.

3. Security issues for the Internet of Things
In today's Internet of Things systems, almost all data is centrally authenticated. If the data passes through a secure channel, the data stream is certified as secure. However, in reality, many Internet of Things systems are directly connected to the Internet, and every data is stored through cloud storage to the data stream. [6]As a result, people or groups with the authority of cloud storage system have the right to access the data stream, or even to unilaterally tamper or delete the data stream. So this kind of data storage is also a problem today.

With the continuous progress of time, the amount of data in this form will be more and more large. If the traditional data storage method is still adopted, the stored data may be attacked by hackers, resulting in the loss of data. For example, we now have a lot of families are using the Internet of things technology door lock, and this kind of lock typically has a password to unlock or fingerprint unlocked two way, a fingerprint to unlock is not very popular reason lies in the fingerprint access numerous and method is relatively simple, so is the password to unlock door locks are widely used in many families, due to the uncertainty and diversity of combination to ensure that the password is not easy to be obtained easily. But whether it is fingerprint lock or password lock, are most of the network function, hackers only need to steal your door lock data, you can easily get the password of your door lock. The existence of this situation has seriously affected our daily life safety.

4. The security of blockchain technology
Blockchain is a decentralized system, which can effectively solve the security problems existing in the Internet of Things.[7-8]Blockchain technology can store the data generated by networking in daily life in an encrypted way, and store and manage the data in a decentralized way, so as to effectively solve the problem of centralized attack system and resist single-point attack mode.

In such an environment, the data generated when users make purchases will be stored in a highly secure manner, which has been recognized in virtual currency transactions, where both parties conduct peer-to-peer transactions without having to go through an intermediate payment system, thus ensuring the security of transactions.

When making a large transaction, due to the uniqueness of blockchain technology, each member of the chain needs to authorize the data, which means all members of the chain must agree to the transaction before the transaction can be completed.

5. Challenges facing blockchain technology
For now, it would be desirable to fully apply blockchain technology to devices that need to be connected to the Internet, but there are still a number of limitations.

Although the technology can effectively guarantee the security of data, it also means that the relevant regulatory authorities cannot effectively supervise the data flow, which leads to the failure to ensure that the transaction is legitimate when conducting transactions. Illegal elements can make use of this particularity to carry out illegal trade for profit activities.

Although this technology can guarantee the security of data, the premise is that the system you use is safe when generating data. If the system is invaded by illegal software or virus to generate data, it will also lead to the loss of data and the data is not complete.[9-10]When clearing the devices in the system, all members in the chain need to be authorized, which is more difficult in reality. (figure 2)
6. Conclusion
The continuous advancement of information technology means that we will produce a large amount of data in our daily production and life. Protecting the security of data is a major problem we are currently facing. The emergence of Blockchain technology allows us to see the dawn in solving this problem. The particularity of Blockchain technology guarantees that our data will not be managed by any central system when stored, which means that peer-to-peer attacks will not affect our data information. The decentralized storage of data in blockchain technology enables us to keep our data information in a more secure environment. Starting from the application of blockchain technology, this paper analyzes the most common identity authentication mechanism in our daily life, analyzes the application of blockchain technology in daily life and puts forward the existing problems from multiple aspects.

References
[1] Sang Anqi, Shen Meng, Zhu Lihuang, et al. A Study on Multi-party Cooperative Security Identity Authentication Mechanism Based on Block-chain [J].; and Journal of Nanjing University of Information Engineering (Natural Science Edition), 2019.
[2] Ma Chenyun. Block chain based multi-party trust authentication method and system :2017.
[3] Xu Jian, Chen Zhide, Gong Ping, et al. Access Scheme for Secure Storage of Medical Records [J.] Based on Block-chain Network Computer applications , 2019,39(5):1500-1506.
[4] Dai Weiguo, Guo Jianqi, Sun Hanbing, et al. A block chain-based authentication method :2020.
[5] Shangguan Lujie. An Analysis of the Application of Block chain Technology in the Field of Network and Information Security [J]. Computer programming skills and maintenance , 2019,000(012):62-64.
[6] Wang Yue. A Study on Customer Certification and Contract Certification Platform Based on Block Chain [J]. Electronic Finance 2019(2).
[7] Zhang Bobo, Zhang Yifeng. A block chain based digital authentication method, device and system :2019.
[8] Wang Bohua, Sun Changjie, Li Zhaochuan, et al. Identity authentication method based on block chain technology [J.] in telecommuting Information Security Research , 2020(4).
[9] Tan Chen, Chen Meijuan, Amuah, et al. A Study on the Identity Authentication Mechanism of Distributed Internet of things Devices Based on Block chain [J].; and Internet of Things Journal, v.4(02): 71-78., 2020
[10] Chen, Zhu Yu, Feng Ke, et al. Identity Authentication of Power System Security and Stability Control Terminal Based on Block Chain J. Journal of Guangxi normal University (Natural Science Edition), 2020(2).

Figure 2. Challenges facing blockchain technology