# Research on Secure Storage of Multimedia Data Based on Block Chaining Technology

Fei Gao[1,2(✉)] and Li Hui Zhen[3]

[1] School of Information Science and Technology, Tibet University, Lhasa 850000, Tibet, China
hl3467985201@163.com
[2] Science and Research Office, Tibet University, Lhasa 850000, Tibet, China
[3] Guangxi Teachers Education University, Nanning 530001, Guangxi, China
gongzuo0758@163.com

**Abstract.** When the traditional multimedia data security storage method is used to store the electronic commerce data, there are some problems such as insufficient security and slow encryption speed, which often lead to data leakage or loss. A secure storage method for multimedia data based on block chain technology is proposed. This method takes the study of multimedia data in the field of electronic commerce as an example. Firstly, the key technology of this method: block chain and multimedia data are introduced briefly, then the block chain of multimedia data is constructed. Finally, a multimedia data storage model of e-commerce is established on the basis of block chain structure. The model is divided into two parts: multimedia data addition Secret and multimedia data preservation. The protection of multimedia data is realized. The results show that compared with the traditional multimedia data security storage method, the security of this method is increased by 15% and the encryption speed is increased by 2 s. It is proved that this method can effectively protect the media data for many years and reduce the frequency of data leakage or loss.

**Keywords:** Block chain · Multimedia data · Secure storage · Four fork tree · Electronic commerce

## 1 Introduction

After the end of the third industrial revolution, computer network information technology was gradually promoted, and digital content based on networks was rapidly developing. So far, more and more data in the party, government, military, and enterprises have emerged in the form of multimedia. Data is no longer confined to written forms, but is preserved in a variety of forms, such as text, video, audio, images, etc. Multimedia data is more intuitive than traditional data, making it easier to query [1]. However, this form of data is also vulnerable to attacks by unauthorized people. Data leakage, data theft, data modification, data deletion, and other situations are not conducive to the safe preservation of data. Therefore, in order to deal with the above problems, there are an endless number of defense methods, such as firewalls and intrusion detection. However, these traditional security defense methods have been


S. Liu and G. Yang (Eds.): ADHIP 2018, LNICST 279, pp. 252–260, 2019.
https://doi.org/10.1007/978-3-030-19086-6_28

difficult to deal with the current threats as the means of illegal intrusion has increased. The existing technologies have obviously insufficient security and defense speed. In view of the above problems, using e-commerce multimedia data information as an example, a method of secure storage of multimedia data based on blockchain technology is proposed [2]. The key point of this method is to encrypt and process multimedia data, without the need of centralized verification, to achieve data security. Firstly, the blockchain technology and multimedia data involved in this method are briefly introduced. Then a blockchain structure of e-commerce data is constructed, and an e-commerce multimedia data storage model is established according to the structure. The model consists of two parts: one uses a quad-tree encoding encryption algorithm to encrypt multimedia data. After the encryption is completed, the encrypted data storage link is entered, and the storage of the encrypted data is implemented in the distributed storage mode to ensure the security of the multimedia data. In order to verify the performance of the multimedia data secure storage method based on blockchain technology, the method test was conducted. The results show that compared with the traditional safe storage method, this method improves the security by 15% and increases the encryption speed by 2 s. This method greatly guarantees the security of multimedia data and reduces the occurrence of data loss and confidentiality events.

## 2 Blockchain Method for Secure Storage of Multimedia Data

### 2.1 Blockchain Technology and Multimedia Data

Blockchain technology, also known as distributed ledger technology, abbreviated as BT, is a technology solution based on Bitcoin, which is a decentralized, high-trust way to collectively maintain a reliable database. Its characteristic is decentralization, openness, consensus mechanism, traceability, and high trust, and is a disruptive information applications following cloud computing, Internet of Things, and Big Data and has been applied in many areas [3]. Figure 1 below shows a typical blockchain.

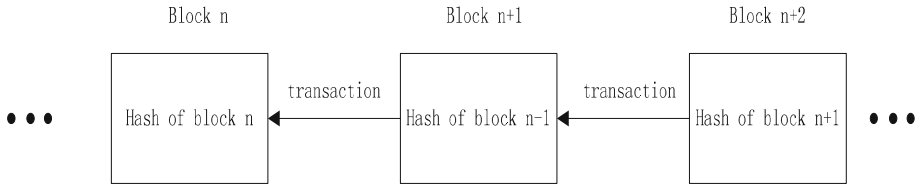


**Fig. 1.** Blockchain

Each block data in the blockchain contains a list of transactions and a hash of the previous block (with one exception, the first block of the blockchain does not contain this hash, called the Genesis Block). Any node in the network can access this ordered, backward-linked data block list, read network transaction data and calculate the status of all transactions in the network. In the blockchain network, all nodes form a peer-to-peer communication network. By copying each node to operate on the same blockchain, its working process is shown in Fig. 2 below.

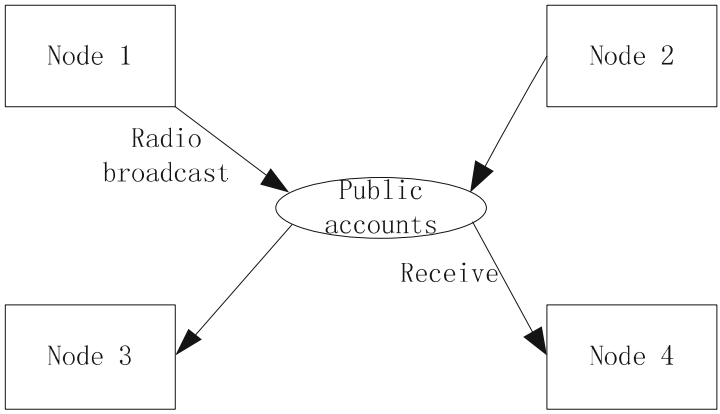


**Fig. 2.** Operation process of block

The above is an iterative process that repeats once every specified time interval. When each node in the network follows the above steps, the shared blockchains that they operate become a network activity record that is verified with time stamp [4].

## 2.2 Construction of Blockchain

The method of secure storage of multimedia data based on blockchain technology is to realize the storage and sharing of e-commerce data records on the basis of blockchain technology and cloud storage technology, and enhance the security and loss prevention of multimedia data. The structure is shown in Fig. 3.

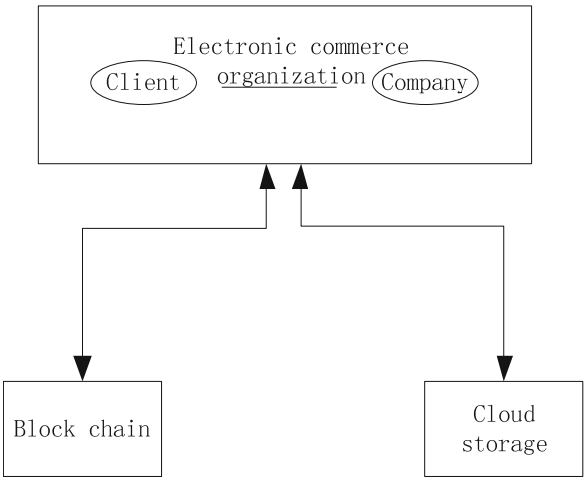


**Fig. 3.** Structure of e-commerce multimedia data blockchain

As it can be seen from Fig. 3, there are three main bodies in the blockchain structure, namely client, electronic commerce organization and company. The client cooperates with the company through the electronic commerce organization, understanding the business and processing through the company to generate multimedia data, data stored in the e-commerce database, the client has the right to use and process personal e-commerce data records, electronic commerce organization and company has the right to query, but can not handle privately. In this blockchain structure, information is shared and can be viewed by the three parties, but relatively private personal information does not appear in its public accounts, but is encrypted and stored in the cloud storage under the chain [5].

### 2.3 Construction of Multimedia Data Storage Model

According to the blockchain structure in Fig. 3, an e-commerce multimedia data storage model is established. The model is mainly composed of two parts: multimedia data encryption and multimedia data storage. The two parts are described in detail below.

**Data Encryption.** In order to ensure the security of multimedia data during transmission and storage, the most commonly used method is to encrypt the data before storing it. At present, there are three types of data encryption algorithms: direct encryption, selective encryption, combination of encryption and compression encoding [6]. In this secure data storage based on blockchain technology, a quad-tree encoding encryption algorithm in combination of encryption and compression encoding process is used to encrypt e-commerce multimedia data. Compared with the former two methods, it has the advantages of fast encrypted speed, high security, and not easy to crack.

Quad-tree encoding is one of the most effective data compression techniques so far. The basic idea is as follows: The multimedia data is recursively partitioned as four quadrants until the value of the sub-quadrant is monotonic, resulting in a reverse quad-tree. To scramble nodes in the same level of the quad-tree structure, the scrambling algorithm is given by:

$$K_H = \left[ \prod_{h=1}^{H} \frac{(N_h + M_h)}{N_{h-1}} \right] \tag{1}$$

Where $K_H$ is the quad-tree with a height of H, H is the height of quad-tree; $N_h$ is the number of internal nodes; $M_h$ is the number of external nodes.

When scrambling the data with Eq. (1), only after more than ten times of repeating scrambling, can the good effect be achieved. And it's obvious that the more the times of scrambling, the more time will be spent by scrambling, the slower the speed of scrambling, the scrambling times should be reduced to improve the scrambling speed, it can be given by Eq. (1):

$$\begin{pmatrix} N_{h+1} \\ M_{h+1} \end{pmatrix} = K \begin{pmatrix} N_h \\ M_h \end{pmatrix} (\mathrm{mod}\, M_h) \tag{2}$$

Therefore, there is matrix K(0), a scrambling is performed by using following Eq. (3), the scrambling effect is equal to that of multi scrambling with Eq. (1):

$$\begin{pmatrix} N_{h+1} \\ M_{h+1} \end{pmatrix} = K \begin{pmatrix} N_h \\ M_h \end{pmatrix} (\mathrm{mod}\, K_0) \tag{3}$$

**Multimedia Data Storage.** After the multimedia data is encrypted, data storage begins. In this link, the database is the carrier of multimedia data information storage, so the design of the database is very important. There are many kinds of multimedia data and the number is huge. Therefore, the database must meet two functional requirements: classifying and storing file information; users can timely and accurately extract the required data information from the database [7]. The data performance needs to be flexible, efficient, safe, reliable, and less redundant. According to the above requirements, part of the database construction code is as follows:

```
<header>
    <div class="container d-flex clearfix">
        <div class="title-box">
            <h2 class="title-blog"> demand analysis
            <ahref="https://blog.csdn.net/huyr_123">HELL
            <p class="description"></p>conception framework design
        </div>
        <div class="opt-box d-flex justify-content-end">
            href="https://blog.csdn.net/huyr_/rss/list">
        </div>
    </div>
</header>
<body>
    <div class="article-info-box">Physical Database Design
        <div class="article-bar-top d-flex24772</span>
    <article>database implementation
        <div id="article_content" class="article_content clearfix
csdn-tracking-statistics" data-pid="blog" data-mod=popu_307 data-dsm =
"post" >database operation and maintenance</div>
    </div>
</body>
end
```

After the database is established, the blockchain stores the multimedia data information in a distributed data storage mode. In each storage operation, the blockchain

takes the previous encrypted data as the basis, and then integrates the data that needs to be stored in the current time to form a new multimedia data. Finally, the blockchain is again quad-tree encoded and encrypted to complete secure data storage. This fact that encryption is performed every time there is new data makes it difficult for the multimedia data in the blockchain to be modified and leaked [8]. In e-commerce data records, there are many image records, such as magnetic resonance imaging, CT, ultrasound, etc. Therefore, in this storage study, only image storage was studied.

After the image data is encrypted, the blocks can be classified according to their different characteristics, such as their colors, effects, and textures. And for fast storage, there must be appropriate index. Index is a structure that sorts the values of one or more columns in a database table. It can be used to quickly access specific information in a database table. In relational database, index is a table-related database structure that can make SQL statements that correspond to tables be executed faster. Table 1 is a typical e-commerce data index.

**Table 1.** E-commerce data index

| Field name | Field type | Length | Explain |
|---|---|---|---|
| ID | Varchar | 8 | Data code |
| NAME | Varchar | 6 | Data name |
| SIZE | Bit | 8 | Data scale |
| Description | Varchar | 5 | Data description |
| Imgurl | Varchar | 7 | Data attachments |
| Abstract Start Date | Text | 4 | Data date |
| Abstract Title | Varchar | 10 | Data title |

## 3 Method Test

In order to test the performance advantage of the multimedia data secure storage method based on blockchain technology designed this paper, a comparative experiment was conducted together with the traditional multimedia data storage method. The experiment is implemented in Matlab environment. The PC is configured as CPU Core i7 3.60 GHz. In the experiment, 90 storage nodes are set. The maximum storage capacity corresponding to each node is 2 TB, and the information data storage channel is 500 Mbit/s. Target information storage and reading information data is 5 TB.

### 3.1 Analysis of Security Test

The security of multimedia data storage is generally expressed by the aggressiveness of the method. Therefore, after using the blockchain technology-based multimedia data secure storage methods and traditional multimedia data secure storage methods to store data, typical operating system attack tools are used for testing. This test is performed mainly through three methods of DoS attacks, virtual machine attacks, and sharing memory attacks. Each attack was performed four times to determine whether the malicious attack was successful. The results are shown in Table 2.

**Table 2.** Comparative analysis results of security

| Name | Secure storage method for multimedia data based on block chain technology | Traditional multimedia data security storage method |
|---|---|---|
| Dos attack 1 | 1 | 1 |
| Dos attack 2 | 1 | 1 |
| Dos attack 3 | 1 | 0 |
| Dos attack 4 | 1 | 1 |
| Virtual machine attack 1 | 1 | 1 |
| Virtual machine attack 2 | 1 | 1 |
| Virtual machine attack 3 | 1 | 0 |
| Virtual machine attack 4 | 1 | 1 |
| Shared memory attack 1 | 1 | 1 |
| Shared memory attack 2 | 1 | 1 |

Note: 0 represents successful attack; 1 represents unsuccessful attack

From Table 2, it can be seen that for the 12 malicious attacks, the method of secure storage of multimedia data based on blockchain technology completely resisted several attacks, did not make illegal access successful, and the security reached 100%. While there are loopholes in traditional multimedia data secure storage methods. For 12 malicious attacks, one Dos attack and one virtual machine attack succeeded, breaking the security line, and the illegal personnel had access to multimedia data. The security was only 85%. Compared with the latter, the former is 15% higher than the latter, which proves that the method of secure storage of multimedia data based on blockchain technology is superior to traditional method of secure storage of multimedia data, which greatly ensures the security of multimedia data and is effective to reduce the occurrence of data loss or leakage events.

### 3.2 Encryption Processing Speed Test Analysis

In Matlab, the encryption speed of the data secure storage method designed in this paper is simulated and tested. Comparison of the encryption speed of two methods with different key lengths is performed to statistically analyze. Table 3 describes the comparison test results of encryption speed of different algorithms.

From Table 3, it can be seen that when the data is 200 bits, 400 bits, and 600 bits, the encryption speed of the two methods are roughly the same. After that, there is a huge gap. As the key length increases, the gap between the two increases. When the key length reaches 2000 bits, the encryption speed of the multimedia data secure storage method based on blockchain technology is 5 s, and the encryption speed of the traditional multimedia data secure storage method is 7 s, and the former is faster than the latter by 2 s.

**Table 3.** Comparison results of encryption speed of two methods

| Key length(bit) | Secure storage method for multimedia data based on block chain technology (s) | Traditional multimedia data security storage method (s) |
|---|---|---|
| 200 | 0.21 | 0.22 |
| 400 | 0.46 | 0.46 |
| 600 | 0.90 | 0.92 |
| 800 | 1.50 | 1.94 |
| 1000 | 2.65 | 3.74 |
| 1200 | 2.89 | 4.60 |
| 1400 | 3.30 | 5.40 |
| 1600 | 4.80 | 6.24 |
| 1800 | 4.96 | 6.53 |
| 2000 | 5 | 7 |

## 4 Conclusion

With the advancement of network information construction, multimedia data information has shown an explosive growth trend, among which confidential multimedia security issues have become increasingly prominent issues, especially e-commerce data, which is the privacy of customers. Related departments have come up with various data secure storage methods to prevent data leakage. Although these traditional methods for secure storage of multimedia data can effectively control the security of confidential multimedia information to a certain extent, as malicious attacks become more and more various, they are gradually becoming inadequate. In such case, the method of secure storage of multimedia data based on blockchain technology is proposed. Compared with the traditional multimedia data secure storage method, this method has improved the security and encryption speed, and basically achieved the purpose of this study.

## References

1. Wen, L.: Spatial data and information fusion in multimedia sensor networks. Comput. Simul. **33**(10), 266–269 (2016)
2. Rui, Q., Shi, D.: Research on the security mechanism of dynamic data storage based on block chain technology. Comput. Sci. **45**(2), 57–62 (2018)
3. Zhenquan, W., Yuhui, L., Jiawen, K., et al.: Smart grid data secure storage and sharing system based on alliance block chain. Comput. Appl. **37**(10), 2742–2747 (2017)
4. Liehuang, Z., Feng, G., Meng, S., et al.: Summary of block chain privacy protection research. Comput. Res. Dev. **54**(10), 2170–2186 (2017)
5. Jiye, W., Lingchao, G., Aiqiang, D., et al.: Research on data security sharing network system based on block chaining. Comput. Res. Dev. **54**(4), 742–749 (2017)

6. Wang, X.: Research on double energy fuzzy controller of electric vehicle based on particle swarm optimization of multimedia big data. Int. J. Mobile Comput. Multimed. Commun. **8**(3), 32–43 (2017)
7. Qingyang, D., Xiuli, W., Jianming, Z., et al.: Information security protection framework based on block chain information physics fusion system. Comput. Sci. **45**(2), 32–39 (2018)
8. Yanxing, Y., Zhou, G.X.: Mass classification of educational multimedia data storage technology research. Modern Electron. Technol. **40**(8), 42–45 (2017)