DIALOGUES WITH SPECIALISTS

Scientific article
UDC 681.3; DOI: 10.61260/2304-0130-2025-1-96-101

DECENTRALIZED INFORMATION STORAGE

✉**Labinsky Alexander Yu.**
Saint-Petersburg university of State fire service of EMERCOM of Russia, Saint-Petersburg, Russia
✉***labinskyi.a@igps.ru***

Abstract. The features and possibilities of decentralized information storage using blockchain technology, an algorithm for implementing a hash function designed to calculate a checksum used to maintain communication between data blocks in a distributed database providing decentralized information storage, are considered.

The problems of distributed database blockchain technology, types of distributed database architectures based on blockchain, and areas of application of blockchain technology are considered.

The cyclic redundancy code algorithm used to calculate a checksum based on input data and the implementation of cyclic redundancy code in the form of a hash function by developing an algorithm and a program for electronic computing machines are considered in detail.

A block diagram of the CRC-32 checksum calculation algorithm and the CRC32 console program implementing this algorithm are presented. An example of calculating a checksum for two lines of text in which the rearrangement of several words led to a change in the checksum is considered.

Key words: decentralized information storage, distributed database, blockchain technology, cyclic redundant code, checksum, hash sum, hash function, algorithm, computer program

For citation: Labinsky A.Yu. Decentralized information storage // Supervisory activities and forensic examination in the security system. 2025. № 1. P. 96–101. DOI: 10.61260/2304-0130-2025-1-96-101.

Introduction

A centralized database assumes that it is hosted on a network node. This architecture is easy to maintain, but it does not provide the necessary level of survivability and timely provision of information services. An alternative to centralization is the distribution of the database in the network, as a result of which each fragment is located in a specific node, which is able to ensure the most efficient use of data [1, 2].

Distributed databases (DDB) can have different architectures that provide decentralized data storage. This article discusses an DDB architecture in which the entire data array is stored as a continuous sequence of data blocks representing a linked list. The relationship between data blocks is maintained by the fact that each block contains its own hash sum and the hash sum of the previous block.

A hash sum is a specific sequence of characters that is always the same for a specific set of data. For identical data, the hash amount is equivalent, which allows you to verify the integrity of files containing information and find errors during data transmission. The hash amount is determined using a special data hashing algorithm that contains a hash function. A hash function converts data of any size into a fixed-length string. In cryptography, the hash amount is used as a data signature (message signature) [3].

Since for the first time decentralized data storage was implemented in the form of a database in the Bitcoin system, such a database is identified with a list (registry) of transactions (groups of operations in databases) in various cryptocurrencies. In 2008, the newly created Bitcoin system implemented for the first time the decentralized storage of information using blockchain technology. In the Bitcoin system, a decentralized database provides storage of all transactions with cryptocurrency [4–6].

Currently, blockchain technologies are used in performing financial transactions, identifying users to access data distributed on a computer network, and developing cybersecurity technologies. Therefore, many banking institutions and government organizations pay attention to the use of blockchain technologies [7].

Let us formulate the problem, the results of which are presented in this article. It is necessary to review the features and capabilities of decentralized information storage using blockchain technology.

The novelty of the research, reflecting the author's personal contribution, is the development of an algorithm for calculating the CRC-32 checksum (hash sum), used to ensure communication between data blocks in the database, and the CRC32 console program that implements this algorithm.

Problems of blockchain technology of distributed databases

There are a number of problems that make it difficult to use blockchain technologies, among which the following are significant [8–9]:

– in the process of use , there is a constant increase in the size of the blockchain files;

– there are limitations on the bandwidth of communication channels between nodes of the distributed blockchain database network;

– there are limitations to the performance of the blockchain.

The last limitation is due to the fact that in the process of operation, certain interaction of the nodes of the blockchain is necessary in order to reach cohesion on the correctness of the information recorded in the next block of the data chain.

Currently, there are three main types of blockchains: public, private, and consortium.

Public blockchains are publicly accessible and maintain user anonymity. They are decentralized and have no administrator. Most cryptocurrencies use public blockchains.

In private blockchains, there is an administrator who has the right to write information to the database blocks. Here, the information gets into the data blocks without delay, since there is no need to reach cohesion on the correctness of the information recorded in the next block of the data chain. This increases the speed of the network. Access to one type of information may be general, while access to another type may be limited.

In consortium blockchains, cohesion and the correctness of information recorded in the next block of the data chain occurs with the help of several predefined network nodes. Such blockchains are considered partially decentralized.

Use of blockchain technology

In addition to cryptocurrencies, the financial sector overall is showing increased interest in blockchain technology. The company was founded by 15 international corporations to create a special platform for the supply of trade in various goods: oil, wheat and etc. [10–11].

VISA, Mastercard, Unionpay, and SWIFT payment systems have announced plans to integrate blockchain technologies [12].

In Russia, VTB and Sberbank banks are showing interest in blockchain technology. In 2017, Alfa-Bank launched a blockchain platform for automating trading operations. In 2021, the concept of «Digital financial assets» was introduced into Russian legislation.

In 2022, the Central Bank of India began using blockchain technologies to make money transfers abroad.

Blockchain technologies have become actively used for identification purposes. Finland uses blockchain technology to identify refugees. In some countries, the blockchain system of electronic citizenship is used. Brazil has an identity card system using blockchain technology.

Blockchain technology can be used to conduct online voting. According to 2020 data, the sectors of the Russian economy using blockchain technologies include: energetics, production and manufacturing, finance and logistics.

Cyclic Redundancy Check

Cyclic Redundancy Check (CRC) This is an algorithm for finding the checksum used to verify data integrity. In practice, cyclic redundant code is implemented as a hash function [3].

The checksum is a number calculated using a specific algorithm based on input data (text messages).

The CRC algorithm is based on the properties of division with remainder of binary polynomials. The CRC (checksum) value is the remainder of dividing the polynomial obtained from the input data by a fixed generating polynomial [3].

The input data is divided into blocks. If the block size is one bit, then the checksum algorithm using such a block is called CRC-1, if the block size is a byte (8 bits), then it is CRC-8, if it is 2 bytes (16 bits), it is CRC–16, if 4 bytes (32 bits), it is CRC-32.

Implementation of the checksum calculation algorithm

The CRC-32 checksum (hash sum) calculation algorithm was implemented as a console program for electronic computing machines (computers). The block diagram of the CRC-32 algorithm of the CRC32 computer program is shown in fig. 1.

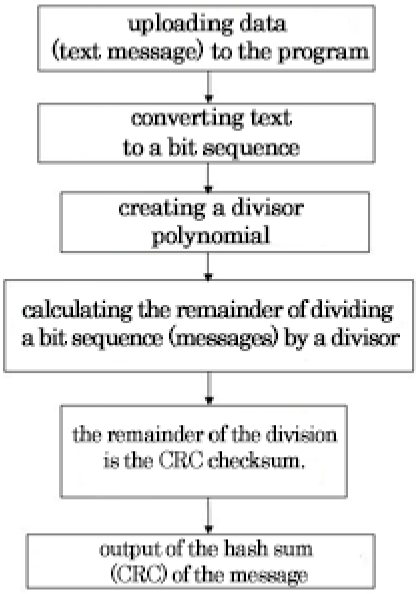
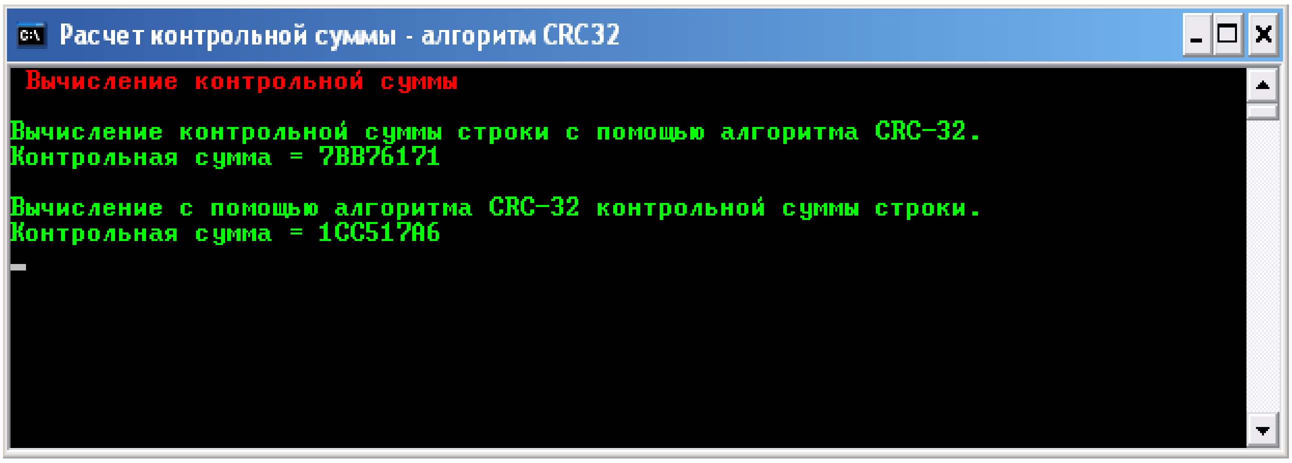


Fig. 1. **A block diagram of the algorithm of the hash sum determination program**

The window of the CRC32 console computer program, which implements the CRC-32 hash sum calculation algorithm, is shown in fig. 2.



```
Расчет контрольной суммы - алгоритм CRC32
 Вычисление контрольной суммы

Вычисление контрольной суммы строки с помощью алгоритма CRC-32.
Контрольная сумма = 7BB76171

Вычисление с помощью алгоритма CRC-32 контрольной суммы строки.
Контрольная сумма = 1CC517A6
_
```

Fig. 2. **The window of the console program for determining the hash amount**

The CRC32 program window shows the result of calculating the checksum (hash sum) for two lines of text: the first line «Calculating the checksum of a string using the CRC-32 algorithm» is the checksum 7BB76171 and the second line «Calculating the checksum of a string using the CRC-32 algorithm» is the checksum 1CC517A6. Rearranging several words led to a change in the checksum.

Conclusion

Over the past few years, blockchain technology in Russia has been used in various sectors of energetics, economics, production and manufacturing, financial and logistics sectors, which justifies the relevance of the topic of the article.

Currently DDB based on the use of blockchain technology are actively used for decentralized data storage. The architecture of the database in question provides for storing an array of data in the form of a continuous sequence of data blocks representing a linked list. The relationship between data blocks is maintained by the fact that each block contains its own hash sum and the hash sum of the previous block.

The CRC-32 algorithm and a console computer program developed by the author are presented as an example of calculating the hash sum.

List of sources

1. Ivanov A.Yu. Mobile distributed databases of automated information and control systems of the EMERCOM of Russia: monograph. SPb.: Saint-Petersburg university of State fire service of EMERCOM of Russia, 2008. 152 p.

2. Raval S. Decentralized applications. Blockchain Technology in Action. SPb.: Piter, 2017. 240 p.

3. Warren G.S. Algorithmic tricks for programmers. M.: Williams, 2007. 288 p.

4. Genkin A.S., Mikheev A.A. Blockchain. How it works and what awaits us tomorrow. M.: Alpina Publisher, 2017. 592 p.

5. Genkin A.S., Mikheev A.A. Blockchain for everyone. How cryptocurrencies and other new financial technologies work. M.: Alpina Publisher, 2023. 588 p.

6. Lelu L. Blockchain from A to Z. All about the technology of the decade. M.: Eksmo, 2018. 256 p.

7. Moghayar U., Buterin V. Blockchain for business. M.: Eksmo, 2017. 224 p.

8. Swan M. Blokcheyn: the scheme of the new economy. M.: Olymp-business, 2017. 240 p.

9. Tabernakulov A., Koifmann Ya. Blockchain in practice. M.: Alpina Publisher, 2019. 264 p.

10. Tapscott A., Tapscott D. Blockchain technology – what is driving the financial revolution today. M.: Eksmo, 2017. 448 p.

11. Haber S., Stornetta W. Blockchain // Journal of cryptography. 2021. Vol. 3. P. 99–111.

12. Nakamoto S. Bitcoin: a per-to-per electronic cash system // Journal of Cryptography. 2019. Vol. 5. P. 37–45.

Information about the article: submitted for editing: 02.02.2025; accepted for publishing: 03.03.2025

Information about authors:
Labinsky Alexander Yu., associate professor of the applied mathematics and information technology chair of Saint-Petersburg university of State fire service of EMERCOM of Russia (196105, Saint-Petersburg, Moskovskiy ave., 149), PhD in technical sciences, associate professor, e-mail: labynsciy@yandex.ru, https://orcid.org/0000-0001-2735-4189, SPIN: 8338-4230