Научная статья

Original article

УДК 004.9.

ИССЛЕДОВАНИЕ ИСПОЛЬЗОВАНИЯ АППАРАТНЫХ РЕСУРСОВ И ПРОИЗВОДИТЕЛЬНОСТИ ХРАНЕНИЯ ДАННЫХ В СЕТИ БЛОКЧЕЙН

RESEARCH ON THE USE OF HARDWARE RESOURCES AND DATA STORAGE PERFORMANCE IN THE BLOCKCHAIN NETWORK

Волков Евгений Алексеевич, магистрант 2 курса ИИКС (Институт интеллектуальных кибернетических систем) Национальный Исследовательский Ядерный Университет «МИФИ»

Дюмин Александр Александрович, доцент кафедры №12 ИИКС (Институт интеллектуальных кибернетических систем) Национальный Исследовательский Ядерный Университет «МИФИ», г. Москва

Volkov Evgeny Alekseevich, eavolkov96@gmail.com

Dyumin Alexander Alexandrovich, eavolkov96@gmail.com

Аннотация. Технологии в наши дни непрерывно развиваются и привносят что-то новое в наши жизни. В современном мире существует быстро развивающаяся и набирающая популярность технология блокчейн. Все в больших масштабах её начинают использовать, и её потенциал признаёт все больше людей и компаний по всему миру. Данная статья призвана не только описать эту технологию с помощью доступных слов и моделей, но и используя наглядные примеры объяснить, что такое блокчейн, и показать

различные сферы применения этой технологии в будущем и настоящем. Кроме того, наша задача показать, почему блокчейн является настоящей революцией в плане хранения и защиты информации.

Annotation. Technology is constantly evolving these days and bringing something new into our lives. In the modern world, there is a rapidly developing and gaining popularity blockchain technology. It is being used on a large scale, and its potential is being recognized by more and more people and companies around the world. This article is intended not only to describe this technology with the help of accessible words and models, but also using illustrative examples to explain what blockchain is, and to show the various fields of application of this technology in the future and present. In addition, our task is to show why blockchain is a real revolution in terms of storing and protecting information.

Ключевые слова: блокчейн, хранение данных, аппаратные ресурсы.

Keywords: blockchain, data storage, hardware resources.

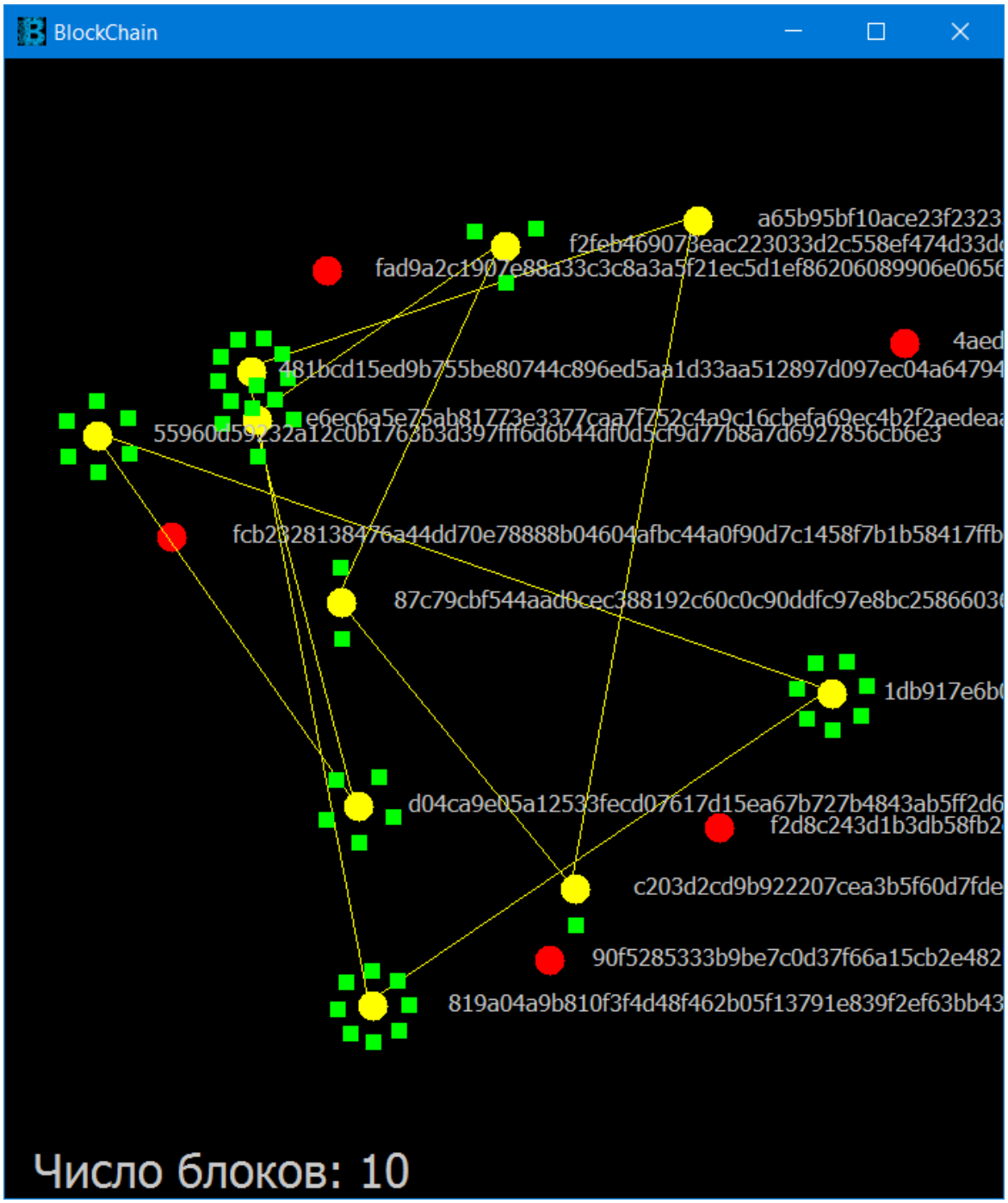
Currently, blockchain technology is used in many areas of business and public administration. Blockchain-based solutions cover financial, government, insurance and other industries where there is an increase in software products implementing this technology. Blockchain is a data structure that allows you to create a digital data registry and share it between a network of independent users.

The main disadvantage of the blockchain is the high consumption of resources. It is necessary to maintain the block chain in real time. Every time a new node is created, it is linked to every other node. This creates transparency. Each node contributes to the level of fault tolerance, and also makes the data stored in the blockchain unchanged. But these actions require the availability of resources, both in terms of network bandwidth and computational resources required to achieve consensus [1, 2].

To test the consumption of hardware resources, a high-level Python implementation of the Blockchain network has been developed, which includes

procedures for creating a new SQLite database, generating a block, writing and reading data, and checking the integrity of the container.

Visualization of the work of the subroutine is shown in picture 1.



Picture 1 – Example of generating ten blocks with the elimination of failed or disabled

When a new block appears in the system and the hash of the new block is stored in all the blocks that are already in the network. When one of the network

participants adds his data, it is transmitted to other network participants. After their placement, information is generated about which of the network participants is their owner. The hash is stored in the database and becomes the hash of a new block of the blockchain network (Table 1).

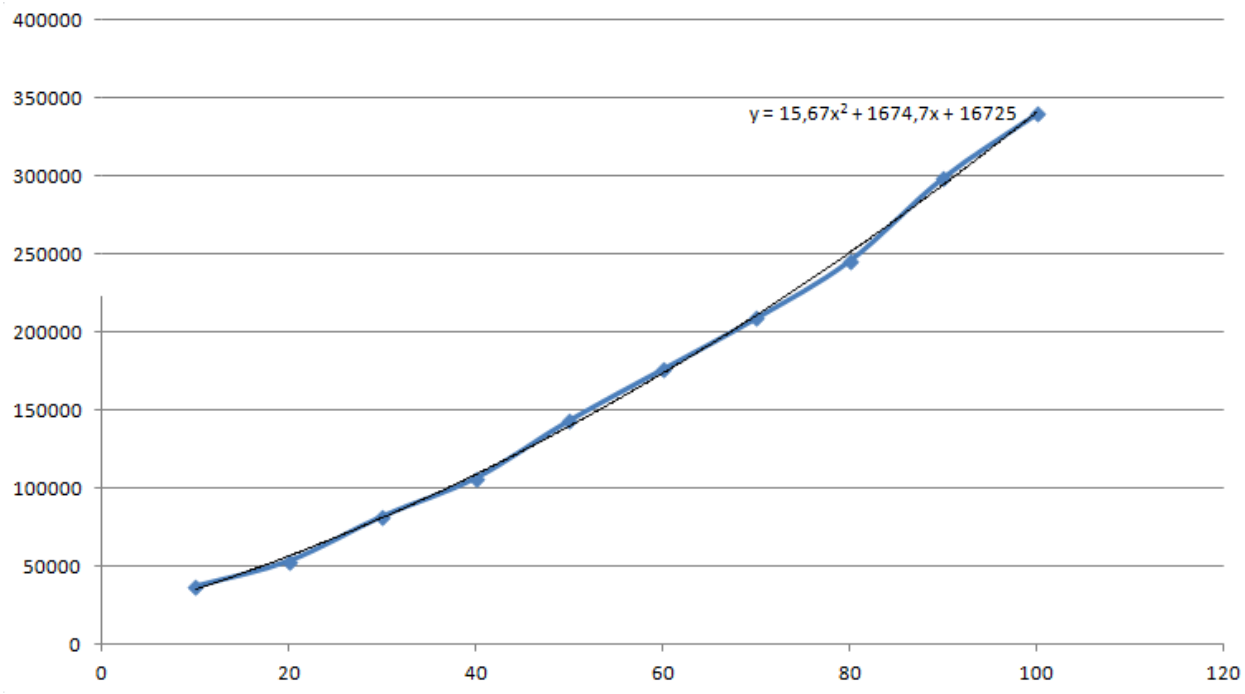
Table 1 – Information about created blocks

Block-Number	BlockHash	Block-Timestamp
1	c77d475c5cded84a7617abbf3bfab51c231809621b8a4be6c9d6a54f80624929	2021-12-22-11.08.27
2	d2c6cd0bb89d7fcff04e130d5ad745c4e06e51c5aff69972017c1a3d2866d600	2021-12-22-11.08.31
3	10951c1c1f4dfb9fb5ff9edf8835553d018e5c471de920451ef0d97d41d4fa90	2021-12-22-11.08.35
4	38eb33136a2b88a808784dc1948e97e9cb3ea611c677a161928a34aa080bd8b0	2021-12-22-11.08.40
5	a41a7a0a189be8d7d0a7d19db39f933a9c77e5f66e27b1e83c8affb18568d731	2021-12-22-11.09.40
6	084b64bd00e961043f765b9b343bf9d06bba0f7c9e343d40da55d8cf73ed0f62	2021-12-22-11.09.46
7	ef6b91f702b7fa7352c72c1008d153868123522ab74273dd6f213f353e721231	2021-12-22-11.10.58
8	49207e10c5159f07304918292ba8dfbfafc68367fe3b7734df7256d0596a30e1	2021-12-22-11.11.38
9	f6131025f65f8b62ba7b1764bd8bdfd665b83ee1870693dccb1349d532212bca	2021-12-22-11.15.03
10	4273e54e10e87abf7f444e514d476952295073ba9769755d53ed497cf5ff3d86	2021-12-22-11.15.11
11	e8ceca5f46133eef25db8e9d76e7d270c090269724310fbe6ad8cd8172acc539	2021-12-22-11.15.26

From the analysis of the model, in particular, the aggregate sizes of SQLite files, we can conclude that the blockchain volume is growing rapidly (Table 2, Figure 2).

Table 2 – Amount of memory for storing blocks

Number of blocks	Amount of storage memory, bytes
10	40 000
20	55 000
30	81 000
40	105 000
50	145 000
60	175 000
70	205 000
80	245 000
90	300 000
100	340 000



Picture 2 – The increase in the amount of memory with an increase in the number of blocks

As a result of approximation of the graph shown in Figure 2 by the trend line, the formula is obtained:

$$y = 15{,}67 \cdot x^2 + 1674{,}7 \cdot x + 16725, \quad (1)$$

where x is the number of blocks, y is the number of bytes of data to store them.

Using the formula (1) describing the growth of data with an increase in the number of blocks, we estimate the volume of a large number of data blocks. The results are summarized in Table 3.

Table 3 – Amount of memory for storing blocks

Number of blocks	**Data volume**				
	Bytes	**Kilobytes**	**Megabytes**	**Gigabytes**	**Terabyte**
100	340895	332,9053	0,325103	0,000317	3,10042E-07
500	4771575	4659,741	4,550529	0,004444	4,33972E-06
1 000	17361425	16954,52	16,55715	0,016169	1,57901E-05
10 000	1,58E+09	1546644	1510,395	1,474995	0,001440425
20 000	6,3E+09	6153819	6009,589	5,868739	0,005731191
50 000	3,93E+10	38338625	37440,06	36,56256	0,035705627
100 000	1,57E+11	1,53E+08	149600,5	146,0942	0,142670148
500 000	3,92E+12	3,83E+09	3736818	3649,236	3,563707075
1 000 000	1,57E+13	1,53E+10	14945674	14595,38	14,25330512
2 000 000	6,27E+13	6,12E+10	59779500	58378,42	57,01017418

Thus, an assessment of the disk space required for storing blockchain data was carried out.

According to Table 3, the number of blocks stored using blockchain technology is about 100 thousand. At the same time , it is required

146 gigabytes of disk space, which, with the modern development of data storage technologies, is a fairly small amount and is available to the average user.

Nevertheless, it is worth noting the nonlinear (quadratic) nature of the growth of the blockchain network, limiting its finite capacity.

To get rid of this disadvantage, so-called Merkle trees are used. Merkle trees are a fundamental part of blockchain technology. The top level of the Merkle tree, the root, arises from a hashing transaction and the pairing of two transactions in nodes located one level below.

The Merkle tree has existed since 1979, when Ralph Merkle, while studying at Stanford, wrote a paper entitled "Certified Digital Signature" [3, 4] and thus created the main component of the blockchain. In his work, Merkle described a completely new method of creating evidence. In fact, Merkle developed a data validation process that would allow computers to process digital signatures much faster.

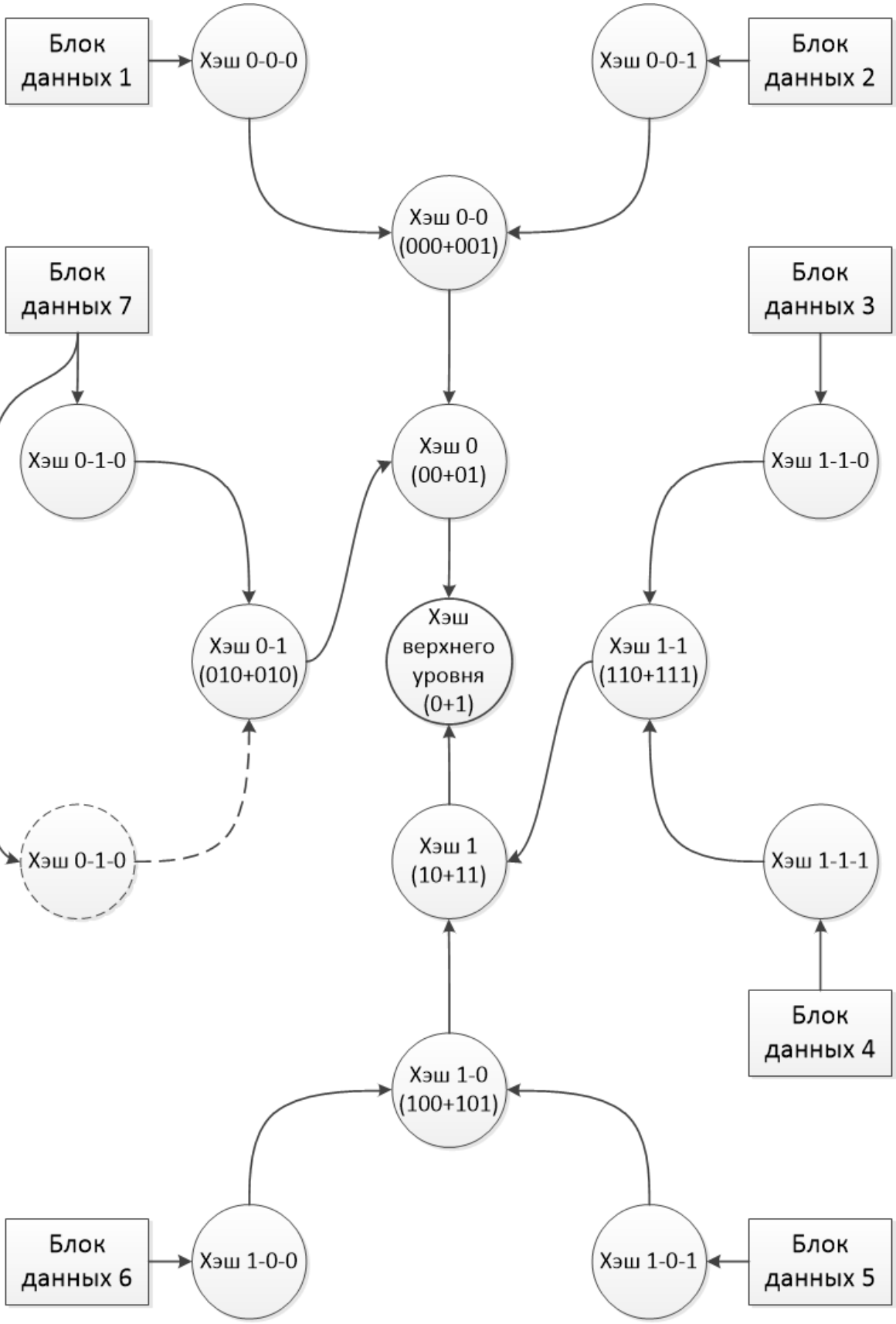
The Merkle tree is constructed as follows (Figure 3):

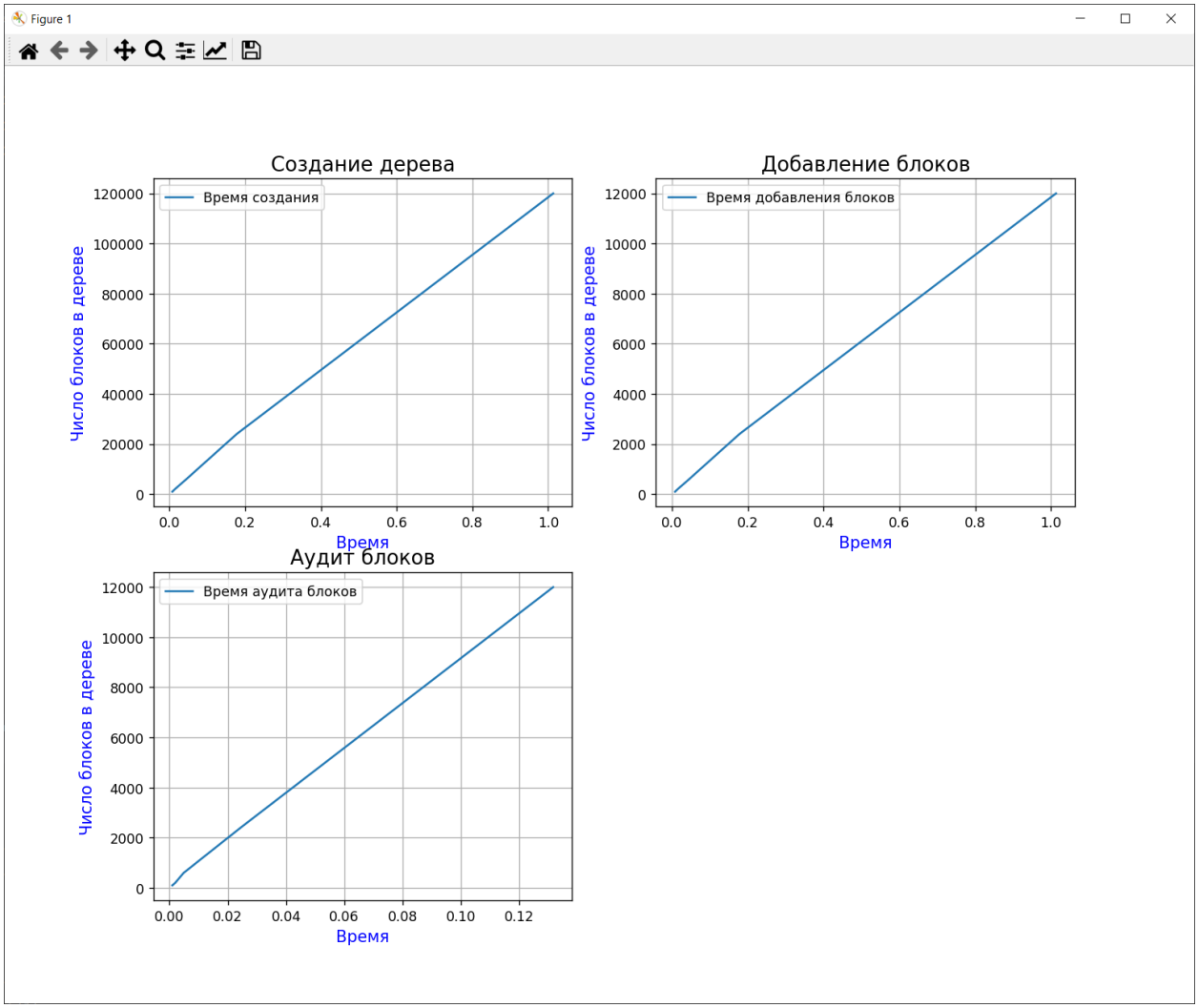
1. The hashes of transactions placed in the block are calculated: hash (Data Block 1), hash (Data Block 2), hash (Data Block 3) and so on.

2. Hashes are calculated from the sum of transaction hashes, for example, hash(hash(Data block 1) + hash (Data block 2)).

3. Then the hash is recalculated from the sum of the hashes. The process is repeated until a single Merkle hash root is obtained. This is a cryptographic proof of the integrity of the block (i.e. that all transactions proceed in the prescribed manner). The root value is set in the block header.

Picture 3 – Building a Merkle tree





Picture 4 – Merkle tree speed test

Conclusions

As a result of studying the system using Merkle trees, linear dependencies of the operating time on the number of packets were obtained, which provides favorable opportunities for system expansion.

Another advantage of the Merkle signature scheme is that it is believed to be resistant to quantum computer algorithms. Traditional public-key algorithms, such as RSA and ElGamal, will become insecure if an efficient quantum computer is created (due to Shor's algorithm [5]). However, the Merkle signature scheme depends only on the existence of reliable hash functions. This makes the Merkle signature scheme very flexible and resistant to quantum computing.

Литература

1. Blockchaintechnology, «Advantages & Disadvantages of Blockchain Technology» : [сайт]. – URL: https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages - disadvantages/
2. Fauvel, W. «Blockchain Advantages and Disadvantages» : [сайт]. – URL: https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0
3. Merkle, R. Secrecy, authentication and public key systems / A certified digital signature. Ph.D. dissertation. / Ralph Merkle // Dept. of Electrical Engineering, Stanford University, 1979.
4. Merkle, R.C. Protocols for public key cryptosystems. In Proceedings of the 1980 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 14—16 April, 1980. p. 122.
5. Описание алгоритма Шора: // Информационная безопасность : [Сайт]. – URL: https://habr.com/ru/post/592413/

Literature

1. 1. Blockchaintechnology, "Advantages & Disadvantages of Blockchain Technology" : [website]. – URL: https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages - disadvantages/
2. 2. Fauvel, W. "Blockchain Advantages and Disadvantages" : [website]. – URL: https://medium.com/nudjed/blockchain-advantage-and-disadvantages-e76dfde3bbc0
3. Merkle, R. Secrecy, authentication and public key systems / A certified digital signature. Ph.D. dissertation. / Ralph Merkle // Dept. of Electrical Engineering, Stanford University, 1979.

4. Merkle, R.C. Protocols for public key cryptosystem. In Proceedings of the 1980 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 14-16 April, 1980. p. 122.
5. Description of the Shor algorithm: // Information security : [Website]. – URL: https://habr.com/ru/post/592413/

© Волков Е.А., Дюмин А. А., Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022.

Для цитирования: Волков Е.А., Дюмин А. А. ИССЛЕДОВАНИЕ ИСПОЛЬЗОВАНИЯ АППАРАТНЫХ РЕСУРСОВ И ПРОИЗВОДИТЕЛЬНОСТИ ХРАНЕНИЯ ДАННЫХ В СЕТИ БЛОКЧЕЙН// Научно-образовательный журнал для студентов и преподавателей «StudNet» №6/2022