DEVELOPMENT AND ANALYSIS OF A BLOCKCHAIN SYSTEM BASED ON JAVASCRIPT

DOI: 10.36724/2072-8735-2021-15-2-40-45

Vasiliy S. Elagin,
SPbGUT, St. Petersburg, Russia,
elagin.vas@gmail.com

Vladimir I. Fedorovskikh,
SPbGUT, St. Petersburg, Russia,
fedorovskih_v@protei.ru

Anastasia V. Spirkina,
SPbGUT, St. Petersburg, Russia,
spirkina.av@gmail.com

Manuscript received 10 November 2020;
Accepted 22 December 2020

The reported study was funded by RFBR, project number 19-37-90050\19

Keywords: *blockchain, JavaScript, distributed databases, data transmission networks, decentralized systems*

The paper describes the main features of blockchain technology, provides the main areas of use of this technology. Today, blockchain has evolved into a reliable and secure way to store and record transactions across a wide range of application domains. However, the impact of existing solutions on the current network infrastructure needs to be considered. The authors propose to create a system for generating and storing blockchain traffic based on the JavaScript programming language. This solution cannot be applied to cryptocurrencies, but it allows you to evaluate the work of a distributed database based on blockchain technology. The aim of the work is to analyze the delays in the generation and distribution of traffic between various numbers of nodes and the dependence of the speed of distribution and block generation on the performance of computers. The paper also considered the algorithm for joining a new node to the cluster and sending a new block to the blockchain, as well as the scheme of a node in a blockchain cluster, and presented the results of an experiment with a quantitative assessment of network performance characteristics.

Information about authors:

Vasiliy S. Elagin*, associate Professor of the Department of Infocommunication systems of SPbGUT, St. Petersburg, Russia*

Vladimir I. Fedorovskikh*, student, Department of Infocommunication systems of SPbGUT, St. Petersburg, Russia*

Anastasia V. Spirkina*, graduate student, Department of Infocommunication systems of SpbGUT, St. Petersburg, Russia*

Для цитирования:

Елагин В.С., Федоровских В.И., Спиркина А.В. Разработка и характеристики блокчейн-системы на языке Javascript // T-Comm: Телекоммуникации и транспорт. 2021. Том 15. №2. С. 40-45.

For citation:

Elagin V.S., Fedorovskikh V.I., Spirkina A.V. (2021) Development and analysis of a blockchain system based on Javascript. *T-Comm*, vol. 15, no.2, pp. 40-45. (*in Russian*)

Introduction

Blockchain is a distributed database that consists of an ever-growing list of structured data, and in this system, data storage and processing devices are not connected to a common server [1-3]. Blockchain is a chain of interconnected blocks formed according to certain principles. Each block contains information about the transaction, as well as additional information, including information about the previous block. Due to this design of the system, it becomes quite difficult to make changes to already existing blocks, since you will have to make changes to the entire subsequent chain [4]. Additionally, blockchain is a decentralized system. This means that the network does not rely on any central trusted authority that can manage the system like traditionally centralized systems. Instead, trust is achieved as an emerging property as a result of interactions between network nodes [5]. At the same time, copies of chains are stored independently on many different computers and servers, which introduces additional difficulties when forging blocks.

Let us present the advantages and disadvantages of this technology [1,6].

Advantages: decentralization; reliability and confidentiality; consensus; transparency of the system and operations.

Disadvantages: scalability; fraud and irreversibility of operations in case of errors; transaction processing speed is lower than in current systems; the possibility of illegal or shady operations.

Initially, the term "blockchain" was applied to the database of the Bitcoin system, because of this, the blockchain is often referred to only for transactions in cryptocurrencies, and there are a large number of them today. However, blockchain can be used in many areas, consider various examples where this technology can be used.

Areas of blockchain application

Today, any payments and transfers require the mediation of a bank or payment system, which require a commission for transactions and establish their own rules and procedures for handling. At the same time, there is the possibility of fraudsters or even the intermediary himself stealing funds from the account. Also, clients may face various failures in the work of the intermediary's information systems or the fact that the intermediary will lose a license for its activities. The blockchain allows you to avoid such situations, in this case all payments and transfers are recorded by several participants in the chain, so that it will not be possible to steal or spend money from the owner's account without a digital signature of the owner himself [7,8]. And with the help of these features of blockchain technology, it became possible to create various cryptocurrencies. Another feature of this technology is the ability to make conditional payments. For example, you can make a payment on the condition that it is made if it is accepted by a user with a private key [9,10]. This, in particular, excludes the possibility of deception when working with fully digital products, such as licenses, videos, music, any kind of access: the buyer will not receive the product if he does not pay, and the seller will not receive money if he does not give the product back. In other variations of the conditions of use are payments "to those who fulfill the conditions of the first", "to someone who has the necessary resources", "to someone who has a certain amount in the account," or other procedure that is easy to perform, but it's hard to fake. Another unusual feature is micropayments, such as time-based payments for watching videos or listening to audio recordings, paying for every ad insert, every click, like, or even emoji.

Blockchain works in bonus programs and loyalty systems. Basically, bonuses work in the same way as money, so all the benefits of blockchain applied to them are valid for bonuses. The consumer can be calm: his savings will not disappear anywhere and will not be spent without his knowledge. In addition, the presence of records gives all participants the opportunity to see the history of the use of bonuses by all participants in the system, and users can be confident in the operation of the blockchain. As for the companies distributing bonuses, they also benefit from using the blockchain. For example, managing the transfer of bonuses to third parties, or controlling and limiting their use for the purchase of certain goods and services.

As mentioned above, the blockchain is highly reliable and secure. Therefore, the technology is perfect for user authentication. The check confirms that the user has an up-to-date and correct key to access the system. Unfortunately, this technology will not be able to protect the owner of the key from his theft more than any other. As you know, the easiest way to get a key from a user is not through hacking, but through social engineering. At the same time, blockchain can protect against penetration into the system and data theft by hacking or deceiving access systems. The distribution of the system makes it practically impossible to break it. An attempted falsification of records will also be quickly exposed due to the fact that only confirmed blocks of records are distributed between users. With the help of blockchain technology, it is possible to create an authentication system for bank customers, which will allow them to securely enter the mobile and Internet bank or perform particularly important transactions in branches. Bank employees can be authenticated in the same way when accessing corporate systems.

The same technology can provide partner banks and technology companies with reliable access to banking systems and data. Another area that requires user authentication and is gaining popularity lately is the Internet of Things [11]. Gradually, it increasingly penetrates into everyday life, and an extraordinary task of authenticating with the participation of inanimate network users appears. For example, the car owner should be given the opportunity to connect to the car, just like the technical support employee; an attacker, on the contrary, should not have such an opportunity. In addition, the owner of the car must connect to his own property, and not to someone else's. A variety of home automation controllers are now in widespread use that control the climate and engineering infrastructure of a home. Many vehicles have systems to monitor driver behavior.

Various sensors and automatic systems have become an integral part of production. However, it's not just humans or machines that need authentication. One of the most natural applications is document authentication. Licenses, rights, certificates, diplomas, contracts, identity cards, reports, extracts, works of art, inventions and discoveries - all this can be recorded in the blockchain.

It is not uncommon for fraudsters to forge collateral assets that do not exist in reality, sell credit cars and mortgage apartments. The peculiarities of blockchain technology make it possible to prevent such vulnerabilities. The technology users have access to the most current and reliable status of the asset, information about who owns it, along with a detailed history of the change of owners, as well as in which existing contracts it participates now and in which already executed contracts it participated in before. Of course, users have the ability to remain anonymous and hide their personal data.

At the same time, they can always check whether they are really dealing with the real owner of the asset and whether he has all the proper rights. It is quite easy to implement this application of the blockchain, since many assets have a unique identifier (registration certificate number, cadastral number, serial number, or even a set of numbers for key nodes and assemblies). This makes even an incomplete ledger, used by only a few participants, useful and beneficial. And then it can be expanded and new users can be easily connected.

An example of blockchain technology implementation in javascript

To implement the blockchain, we need several devices (for this implementation we will use two devices), since the blockchain is, in fact, a distributed database supporting a growing list of blocks. Within the framework of this paper, the blockchain will be created not for the formation of cryptocurrencies or smart contracts, but for the sake of studying the blockchain itself.

To organize a blockchain system, it is proposed to use the JavaScript language, the ECMAScript 6 standard.

Requirements for our system:

1. Control of nodes via HTTP interface;
2. Using Websocket between nodes for communication (P2P);
3. "Protocols" for P2P communication should be simple;
4. Data is not stored on nodes;
5. No proof of work performed.

Block structure

For clarity, and based on the purposes of the study, we will add data, indices, timestamps, the hash of the block itself and the hash of the previous block to the block [6-8].

```
class Block {
    constructor(index, prevHash, timestamp, date, hash) {
        this.index = index;
        this.prevHash = prevHash.toString();
        this.timestamp = timestamp;
        this.data = data;
        this.hash = hash.toString();
    }
}
```

The hash sum is required to maintain the integrity of the blocks and data contained in the blockchain. In this system, the SHA-256 algorithm will be used for hashing.

```
var calcHash = (index, prevHash, timestamp, data) => {
    return CryptoJS.SHA256(index + prevHash + timestamp +
data).toString();
};
```

To generate a block, we need to find out the hash of the previous block and add the necessary elements to the block structure – data, timestamp, index and hash sum.

```
var genNextBlock = (blockData) => {
    var prevBlock = getLatestBlock();
    var nextIndex = prevBlock.index + 1;
    var nextTimestamp = new Date().getTime() / 1000;
    var nextHash = calcHash(nextIndex, prevBlock.hash,
nextTimestamp, blockData);
    return new Block(nextIndex, prevBlock.hash,
nextTimestamp, blockData, nextHash);
};
```

We will use an array to store blocks. The first block is created by hand, its name is "genesis block".

```
var getGenesisBlock = () => {
    return new Block(0, "0", 1590761001, "genesis block is
the first block", "
d4c5ff971e067e3233c4c2d0083286736b75e25933e04a659c3c33
e9134a20f9");
};
var blockchain = [getGenesisBlock()];
```

Before receiving new blocks for storage from other nodes, it is necessary to be able to confirm the integrity of the received block (or block chain).

```
var checkValidNewBlock = (newBlock, prevBlock) => {
    if (prevBlock.index + 1 !== newBlock.index) {
        console.log('Wrong index');
        return false;
    } else if (prevBlock.hash !== newBlock.prevHash) {
        console.log('Wrong  hash of previous block');
        return false;
    } else if (calcHashForBlock(newBlock) !==
newBlock.hash) {
        console.log('Wrong hash: ' +
calcHashForBlock(newBlock) + ' ' + newBlock.hash);
        return false;
    }
    return true;
};
```

In any case, the sequence of blocks in the chain must be specified explicitly, so that when a conflict occurs (for example, two nodes simultaneously generate blocks with the same index), we choose the chain containing the largest number of blocks.

```
var replaceChain = (newBlocks) => {
    if (checkValidChain(newBlocks) && newBlocks.length >
blockchain.length) {
        console.log('The accepted blockchain is valid. The current blockchain is being replaced with a new one.');
        blockchain = newBlocks;
        broadcast(responseLatestMsg());
    } else {
        console.log('The accepted blockchain is not valid.');
    }
};
```

An integral part of any blockchain is a distributed database. To maintain this architecture, nodes must communicate with each other. Let's define the rules for network synchronization:

1. When generating new blocks, the node must inform the network about this event;
2. When connecting to a new node, information about the last generated block is requested;
3. When a block comes to a node with an index greater than that stored in it, then the block is either added or complete information about the block is requested.

It should be noted that the search for nodes does not automatically occur in the available network, all links are added manually.

Site owners should be able to control their site, this is solved through the installation and correct configuration of the HTTP server.

The following functions must be available to the user:

1. Viewing the list of blocks;
2. Generation of a block with content;
3. Viewing and editing the list of peers

The easiest way to communicate is with curl:

```
# list all blocks on a node
curl http://127.0.0.1:8080/block_list
```

It should be noted here that the nodes address not one, but two HTTP servers: one for user control over the node, and the second for Websocket HTTP when establishing a P2P connection between the nodes.

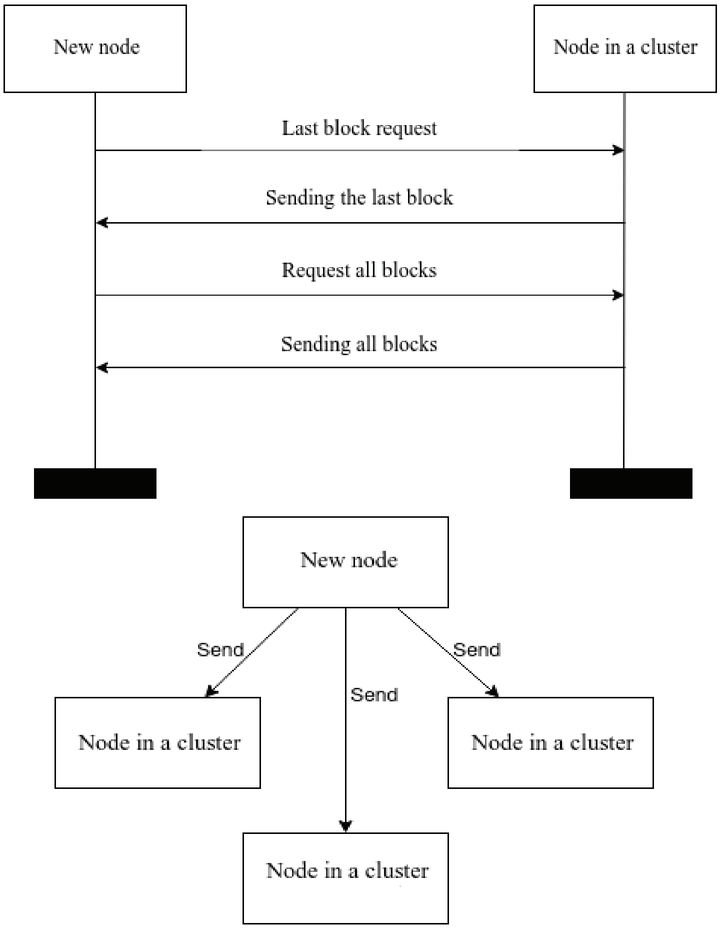

Fig. 1. A new node joins the cluster and sends a new block to the blockchain

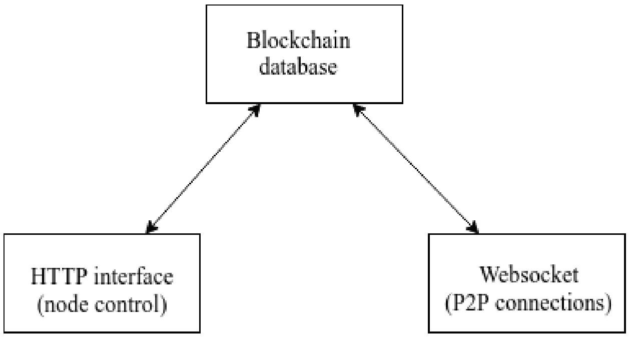

Fig. 2. Scheme of a node in a blockchain cluster

Analysis of block transmission delays

One of the main disadvantages of P2P blockchain is the high latency in the transfer of blocks when the number of nodes is large enough. During the analysis, statistics were collected on the delays between the transmission and reception of blocks in the network.

The main tool for analyzing statistics is the histogram of the distribution of the estimated random variable [15]. In the course of the analysis, a network of local and remote nodes (10 local and 1 remote) was created, the timestamps of sending and receiving blocks (at least 100) with data (in ms) were collected with the simplest Bash scripts. Further, based on these time stamps, we divided the obtained values into several intervals and calculated how many packets from our sample fell into each range. By displaying these values in the form of vertical "bars", one can obtain the distribution histograms shown in Figure 3 and Figure 4.

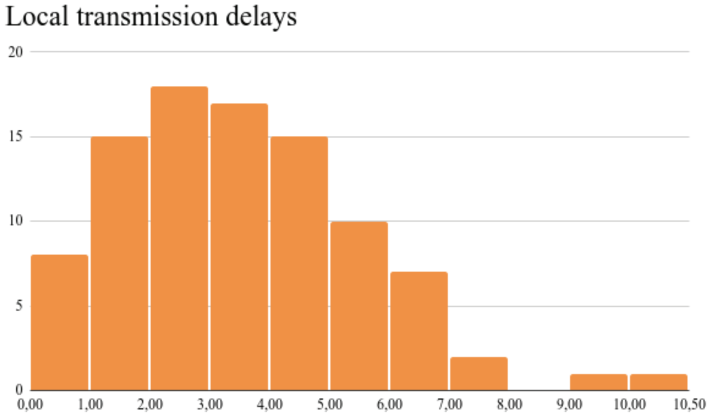

Fig. 3. A histogram of node latency distribution located locally (on the same server as the block sender)

A histogram of latency distribution gives a good indication of the health and performance of the network. Based on this data, you can judge which levels of latency are more likely and which are less. The more results we analyze, the with a higher degree of confidence we can predict delays in a given network in the future.

Further, using statistical analysis and mathematical apparatus, several main characteristics of the performance of the blockchain network were calculated, and are presented in Table 1.

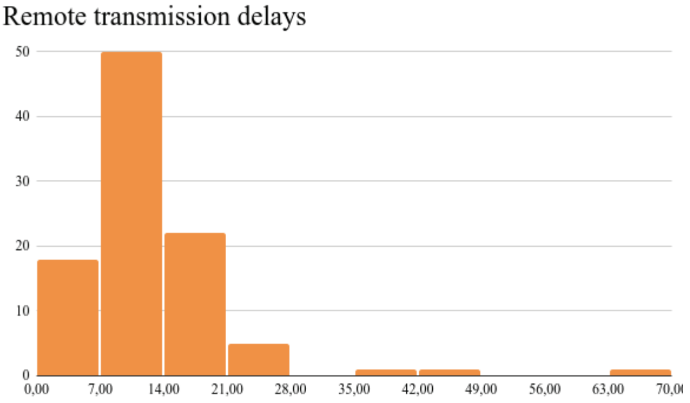

Fig. 4. A histogram of node latency distribution located remotely (on different servers with the block sender)

Table 1

Performance characteristics of the blockchain network

	Local	Remote
Average delay value, ms	3,49805	12,41991
Median, ms	3,28625	10,47415
Standard deviation, ms	2,02066	8,72470
The coefficient of variation	0,57765	0,70247

Statistical analysis showed that for nodes located remotely in relation to nodes located within the same local network, the values of the mathematical component of the delay increased, the average value was 3.5 times, the median was 3.2 times, the standard deviation was 4 times, and the coefficient variations 1.2 times.

From the results in Table 1, we can conclude that the delay values for both variants of the location of the nodes are a combination with a large fluctuation, and the spread of values is large.

Conclusions

Blockchain is a distributed ledger technology that has grown in importance since its inception. In addition to cryptocurrencies, it has also expanded its boundaries, inspiring various organizations, businesses or commercial institutions to implement this technology using the most innovative security features. Decentralized and immutable aspects were the key points that confirm that blockchain is one of the most secure technologies at present [16]. Since blockchain users cannot change the transaction history, this requires changing the blockchain at each node. Of course, any system is not without its drawbacks, like blockchain. For example, the speed of data update. If we take the simplest structure, as in the presented blockchain, when each node accesses each node (P2P), then the block propagation speed decreases with an increase in the number of nodes in the network. In more complex systems, much more complex algorithms for selecting peers with ranking and so on are implemented. Another disadvantage is that each node must store the entire data chain. In large systems, this is solved by the fact that there are data storage systems where the entire volume of the database is stored, and users who store only the amount they want, depending on the storage time or volume. As a result, we get that the main idea of the blockchain and the main area where it can be applied is confirmation of facts (transactions, actions, etc.) in a situation where everyone does not trust everyone. In these conditions, the blockchain performs very well, because all transactions are transparent.

In this paper, the authors have developed a blockchain system and conducted a number of experiments, the results obtained a histogram of the distribution of delays at a node located locally and a histogram of the distribution of delays at a node located remotely. It should be noted that the results obtained in the course of the current experiment coincide with the results in studies that conducted full-scale controlled experiments, for example, in [3]. That allows you to judge the correctness of the model and the correctness of writing the code.

In further work, it is planned to refine the code and provide broader and more unified possibilities of using the system, which can be applied to all or limited types of blockchain at the user's request. It is also planned to conduct a number of experiments to assess the various characteristics of the system and the dependence on various network situations.

References

1 W. Mougayar (2016). The business blockchain, New Jersey: John Wiley & Sons Inc., Hoboken.

2 A.B. Goldstein, N.A. Sokolov, V.S. Elagin, A.V. Onufrienko and I.A. Belozertsev (2019). Network Characteristics of Blockchain Technology of on Board Communication. *2019 Systems of Signals Generating and Processing in the Field of on Board Communications*, Moscow, Russia, pp. 1-5, March 20-21.

3 V. Elagin, A. Spirkina, A. Levakov, I. Belozertsev (2020). Blockchain Behavioral Traffic Model as a Tool to Influence Service IT Security. *Future Internet 2020*, 12, 68.

4 X. Li et al. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems*. Vol. 107. P. 841-853.

5 A.M. Antonopoulos (2017). Mastering Bitcoin, O'Reilly Media Inc.: Sebastopol, CA, USA.

6 V.S. Elagin, A.V. Spirkina, A.G. Vladyko, E.I. Ivanov, A.V. Pomogalova, E.A. Aptrieva (2020). The main network characteristics of blockchain traffic and approaches to modeling. *T-Comm*. Vol. 14. No.4.

7 L. Carlozo (2017). What is blockchain? Journal of Accountancy. Vol. 224. No. 1. P. 29.

8 D. Yaga et al. (2019). Blockchain technology overview. *arXiv preprint arXiv*:1906.11078.

9 T. Ahram et al. (2017). Blockchain technology innovations. *2017 IEEE technology & engineering management conference (TEMSCON)*. IEEE. P. 137-141.

10 M. Risius, K. Spohrer (2017). A blockchain research framework. *Business & Information Systems Engineering*. Vol. 59. No. 6. P. 385-409.

11 A. Pieroni, N. Scarpato, L. Felli. Blockchain and IoT Convergence – A Systematic Survey on Technologies, Protocols and Security. *Appl. Sci*. 2020, 10, 6749.

12 P. Narayan (2018). Blockchain. Application Development.

13 Blockchain in 200 lines of code. [Electronic resource]. access mode: https://habr.com/ru/post/323586/ (date of treatment 06/23/2020)

14 S. Bikramaditya, D. Gautam, P. Panda. Blockchain (2020). A guide for beginner developers. BHV.

15 To the calculation of the characteristics of systems with a limited number of load sources. (Abstracts). *Scientific and technical conference of the faculty, researchers and graduate students of St. Petersburg State University of Technology*. Materials of the conference SPb.: 2009.

16 S. Sayeed, H. Marco-Gisbert (2020). Proof of Adjourn (PoAj): A Novel Approach to Mitigate Blockchain Attacks. *Appl. Sci*., 10, 6607.

РАЗРАБОТКА И ХАРАКТЕРИСТИКИ БЛОКЧЕЙН-СИСТЕМЫ НА ЯЗЫКЕ JAVASCRIPT

Елагин Василий Сергеевич, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,* **elagin.vas@gmail.com**

Федоровских Владимир Игоревич, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,* **fedorovskih_v@protei.ru**

Спиркина Анастасия Валентиновна, *Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича,* **spirkina.aa@gmail.com**

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 19-37-90050/19

Аннотация

В данной статье описываются основные особенности технологии блокчейн, приводятся основные сферы использования данной технологии. Сегодня блокчейн превратился в надежный и безопасный способ хранения и записи транзакций в широком спектре доменов приложений. Однако необходимо рассмотреть влияние существующих решений на текущую сетевую инфраструктуру. Авторами предлагается создание системы для генерации и хранения блокчейн трафика на основе языка программирования JavaScript. Данное решение не может быть применимо для криптовалют, но оно позволяет оценить работу распределённой базы данных на основе технологии блокчейн. Целью работы является анализ задержек при генерации и распределении трафика между различным количеством узлов и зависимость скорость распределения и генерации блоков от производительности компьютеров. Рассмотрен алгоритм присоединения нового узла к кластеру и отправки нового блока в блокчейн, а так же схема узла в кластере блокчейн и представлены результаты эксперимента с количественной оценкой характеристик производительности сети.

Ключевые слова: *блокчейн, JavaScript, распределенные БД, сети передачи данных, децентрализованные системы.*

Литература

1. *Mougayar W.* The business blockchain, New Jersey: John Wiley & Sons Inc., Hoboken, 2016.
2. *Goldstein A.B., Sokolov N.A., Elagin V.S., Onufrienko A.V., Belozertsev I.A.* Network Characteristics of Blockchain Technology of on Board Communication // 2019 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia, 2019, pp. 1-5, March 20-21.
3. *Elagin V, Spirkina A., Levakov A., Belozertsev I.* Blockchain Behavioral Traffic Model as a Tool to Influence Service IT Security // Future Internet 2020, 12, 68.
4. *X. Li* et al. A survey on the security of blockchain systems // Future Generation Computer Systems. 2020. Т. 107. С. 841-853.
5. *Antonopoulos A.M.* Mastering Bitcoin, O'Reilly Media Inc.: Sebastopol, CA, USA, 2017.
6. *Елагин В.С., Спиркина А.В., Владыко А.Г., Иванов Е.И., Помогалова А.В., Антриева Е.А.* Основные сетевые характеристики blockchain трафика и подходы к моделированию // T-Comm: Телекоммуникации и транспорт. 2020. Т. 14. № 4. С. 39-45.
7. *Carlozo L.* What is blockchain? // Journal of Accountancy. 2017. Т. 224. №. 1. С. 29.
8. *Yaga D.* et al. Blockchain technology overview // arXiv preprint arXiv:1906.11078. 2019.
9. *Ahram T.* et al. Blockchain technology innovations // 2017 IEEE technology & engineering management conference (TEMSCON). IEEE, 2017. С. 137-141.
10. *Risius M., Spohrer K.* A blockchain research framework // Business & Information Systems Engineering. 2017. Т. 59. №. 6. С. 385-409.
11. *Pieroni A., Scarpato N., Felli L.* Blockchain and IoT Convergence-A Systematic Survey on Technologies, Protocols and Security // Appl. Sci. 2020, 10, 6749.
12. *Нараян П.* Блокчейн. Разработка приложений, 2018 г.
13. Блокчейн в 200 строк кода. [Электронный ресурс]. - режим доступа: https://habr.com/ru/post/323586/ (дата обращения 23.06.2020)
14. *Бикрамадитья С., Гаутам Д., Панда П.* Блокчейн. Руководство для начинающих разработчиков, BHV, 2020 г.
15. К расчету характеристик систем с ограниченным числом источников нагрузки. (Тезисы). // 61 Научно-техническая конференция профессорско-преподавательского состава, научных сотрудников и аспирантов СПбГУТ. // Материалы конференции СПб.: 2009.
16. *Sayeed S., Marco-Gisbert H.* Proof of Adjourn (PoAj): A Novel Approach to Mitigate Blockchain Attacks // Appl. Sci. 2020, 10, 6607.

Информация об авторах:

Елагин Василий Сергеевич*, к.т.н., доцент кафедры Инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, СПбГУТ, г. Санкт-Петербург, Россия*

Федоровских Владимир Игоревич, *кафедра Инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, СПбГУТ, г. Санкт-Петербург, Россия*

Спиркина Анастасия Валентиновна, *аспирант, кафедра Инфокоммуникационных систем Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, СПбГУТ, г. Санкт-Петербург, Россия*