А. Ю. Попадюк [A. Yu. Popadyuk],
Е. К. Коровяковский [E. K. Korovyakovskiy]

УДК 519.246.8

АНАЛИЗ ОТКРЫТОГО БЛОКЧЕЙНА В РАМКАХ КОМПЛЕКСНОЙ КЛАССИФИКАЦИИ ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА

ANALYSIS OF PUBLIC BLOCKCHAIN UNDER THE COMPLEX CLASSIFICATION OF SHARED LEDGER TECHNOLOGY

Петербургский государственный университет путей сообщения Императора Александра I, Санкт-Петербург, Россия / Emperor Alexander I St. Petersburg State Transport University, St. Petersburg, Russia

Аннотация. *В статье ставится задача произвести анализ открытого блокчейна в рамках предложенной автором комплексной классификации технологии распределенного реестра. В ходе решения указанной задачи автор определяет ключевые свойства, присущие публичным блокчейнам, описывает характерные открытым реестрам алгоритмы консенсуса, а также определяет основные достоинства и недостатки таких систем. В заключении предложены рекомендуемые области применения открытых распределенных реестров.*

Ключевые слова: блокчейн, распределенный реестр, прозрачность, логистика, децентрализация, криптовалюта, биткоин, цифровизация.

Abstract. *The object of the article is an analysis of public blockchain under the complex classification of* shared *ledger technology suggested by the author. The author defines the key properties of the public blockchains, the consensus algorithms and he finally determines the advantages and disadvantages of the open shared ledgers in the course of task performance. The recommended fields of application are suggested in the conclusion.*

Key words: blockchain, shared ledger, transparency, logistics, decentralization, cryptocurrency, bitcoin, digitization.

Introduction. According to the complex classification of the shared ledger technology proposed by the author, there are four types of blockchain systems, each of which has unique properties (Fig. 1). An important role in the process of data transmission and storage is played by public blockchains, which ensured the successful integration of shared ledger technology into modern business processes.

Materials and methods, results and discussions. Currently, there are public & open blockchains, which have the most free level of access and provide users with ample opportunities for organizing operations performed within the network, and public & closed blockchains, where, with free access, user rights are limited by solving some of the problems of open blockchain systems.

Public & open blockchains are immutable, pseudo-anonymous (or anonymous), and decentralized systems. This means that anyone can become part of the network and take part in the consensus process. These systems have the properties of resistance to censorship and protection of transactions from retrospective changes, which makes it possible to ensure the reliability of the content of the blockchain even in the absence of trust between the participating objects. In addition, thanks to the public access to the platform, all processes occurring within the network are completely transparent.

The main advantage of public & open blockchains is an increased level of system security due to the use of the Proof-of-Work consensus algorithm. Thus, the process of confirming transactions when using the specified algorithm is as follows[32]: miners (persons who verify and confirm user transactions) observe the transactions broadcast to the network and add them to their pool. Due to the large number of unconfirmed transactions and the limited block size[33], miners are forced to select the most priority ones, primarily focusing on the size of the commission offered by the user for adding to the block. As soon as the transactions are collected, the computing power of all miners automatically starts performing the most complex mathematical tasks in order to determine the hash value of the new block.[34] First of all, the validity of each transaction of the block is checked for the presence of the funds specified for the transfer by the senders, after which a "Merkle tree" is formed with correct transactions. To build a "Merkle tree", each transaction located in the miner's pool is hashed. The resulting hash values are then combined in pairs and re-hashed. This algorithm runs until the resulting hash value is determined, also known as the "Merkle root" (Figure 2).

[32] On an example of the Bitcoin blockchain

[33] Each block in the Bitcoin blockchain has a size limit of 1 megabyte to protect the blockchain from malicious attempts to disable the blockchain using DDos attacks.

[34] Hashing is the process of converting input information into a fixed-length encrypted code. Accordingly, the hash value is information contained in a block, encrypted with the SHA-256 cryptographic function in order to be able to determine the integrity of the information and uniquely identify the specified block.

public & open blockchain	public & closed blockchain
• Anyone can join • Anyone can read, write and confirm transactions • Hosted on public servers • Low scalability	• Anyone can join • Anyone can read • Only authorized participants can write and confirm transactions • Medium scalability
privite& open blockchain	**privite & closed blockchain**
• Only authorized participants can join • Only authorized members can read and write • Hosted on private servers • High scalability	• Only authorized participants can join • Only authorized members can read • Only the network operator can write and confirm transactions • Very high scalability

Fig. 1. Types of blockchain networks

The next piece of mathematical calculations is the process of finding a nonce – a random number given by the system. In connection with security issues, the blockchain automatically sets the complexity of the cryptographic task of finding a hash in such a way that the average time to determine it is 10 minutes. For example, the system can set the following condition: the hash function of the new block must start with three zeros in a row. Depending on the set complexity, the number of zeros at the beginning of the function can vary in different directions.

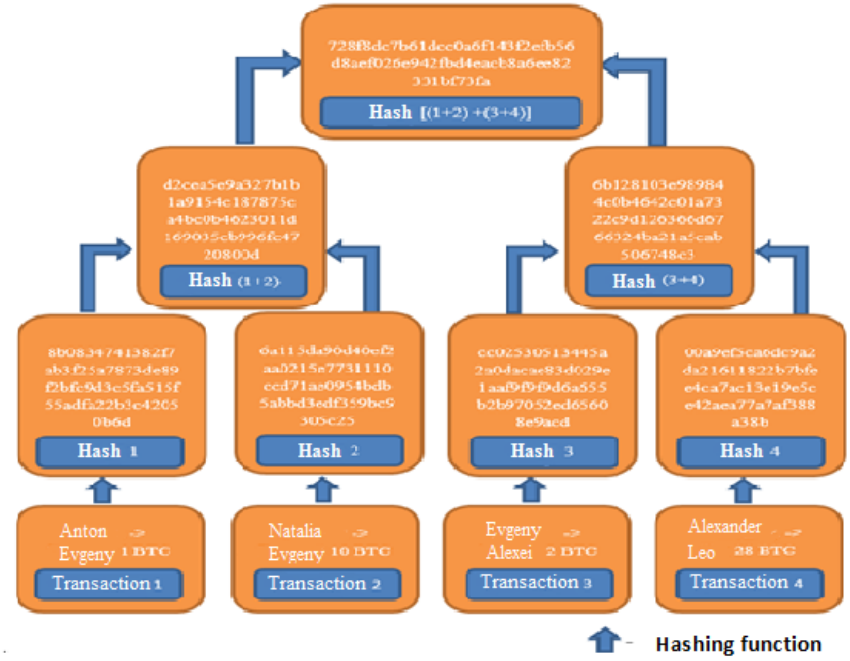

Fig. 2. "Merkle tree" in the presence of 4 transactions in the block

The nonce search process does not have a mathematical algorithm, therefore, it is performed by iterating over the values. The *miner*, whose computer power is the first to detect the specified *nonce* and determine the hash function of the new block, automatically sends the received response to all network nodes in order to confirm the work done. Thus, the generated block joins the existing blockchain, and *miners* proceed to create the next block [1]. The blockchain structure in the blockchain is shown in Figure 3

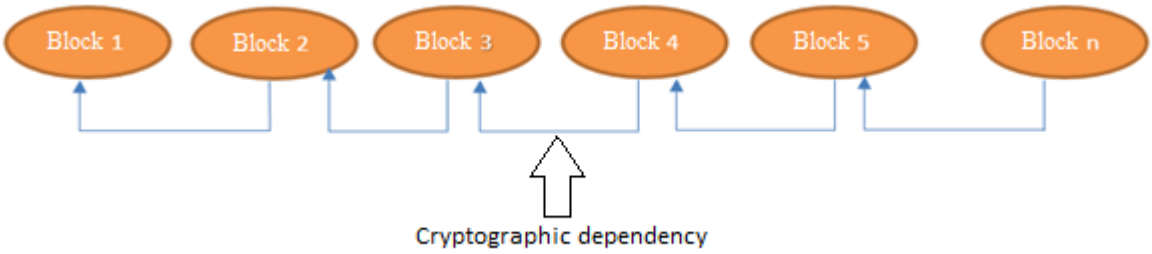

Fig. 3. Block sequence in the blockchain

Each subsequent block in the shared ledger is cryptographically linked to the previous block, thus creating a secure chain. If an attacker tries to change the transaction data contained in a block (for example, the amount of money transfer), the cryptographic relationship of the specified block with the rest of the chain will be broken, which will lead to the sequential destruction of all further blocks (Fig. 4)

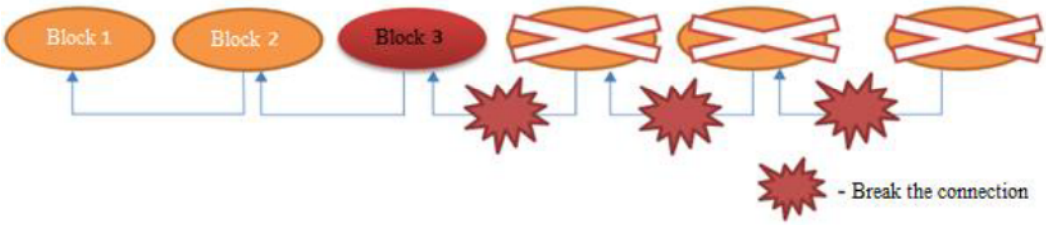

Fig. 4. An attempt to change the data in block 3

It should be mentioned that the blockchain has a "long chain" rule. Namely, the chain of blocks, which is the longest, is taken as the only correct version of the existing system, and, accordingly, all further generated blocks will be added to this chain. Thus, in order for the community to recognize the changes of the attackers as true, the attackers need to determine the hash values of all subsequent blocks and continue creating new blocks in their chain faster than all the miners of the network working in the original version of the blockchain will do (Figure 5).

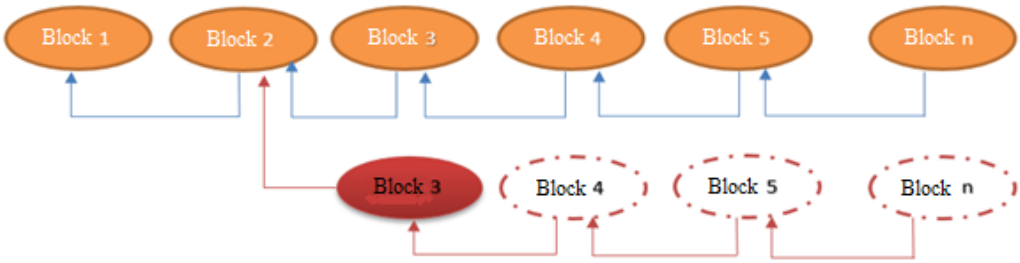

Fig. 5. Creation of an alternative chain as a result of the attack on block 3[35]

This task is practically impossible due to the need for more than 50% of all existing computer power in the hands of attackers. Even if the specified condition is met, such an attack would be inappropriate due to the high monetary costs associated with increased power consumption in the mining process. In addition to financial costs, there are significant time costs. The older the transaction, the more computing it will take to successfully attack it. A transaction with an age of 1 year will require an attacker about 1 year of computation, provided that the attacker's hash[36] rate is twice the hash rate of all other *miners*. Thus, this algorithm successfully ensures the security of the system. The disadvantages of the proof-of-work consensus algorithm include low bandwidth. Due to the need to confirm all transactions by each node in the network, scalability problems arise for such blockchains. Thus, the throughput of the Bitcoin blockchain is 7 transactions per second, while the Visa payment system processes up to 24,000 transactions per second[37] [3]. There is also a problem of increased power consumption arising from the need to perform computer calculations to confirm transactions and reach consensus. According to a report by the British agency *PowerCompare*, the total amount of electricity spent on mining exceeds the energy consumption of 159 countries around the world. Every year, as a result of the mining process in Russia, 1.065 trillion. kW / year, which negatively affects the country's ecology [4].

[35] In fact, one block can contain not 4, but 4000 transactions.
[36] Hashrate - the number of attempts per second to find the correct nonce value [2]
[37] It should be noted that scientists are actively working on solving the problem by introducing «sharding» и «lightningnetwork» technologies into the blockchain, but the final results have not yet been presented.

In addition to enhanced security, public & open blockchains offer no infrastructure costs to build and run decentralized applications (dApps). Such systems are completely open and transparent for all network participants, and transactions in them are unchanged. Confirmed transactions are replicated to each participating node, while consensus takes care of validating and synchronizing them, allowing users to transact with trust in the system. Although transactions can be read by anyone, user identities are protected to ensure their anonymity. Among the main disadvantages of an public & open blockchain, the following properties should be highlighted:

1) Limited scalability (there is a limit on the number of transactions that can be created during periods of increased network load).

2) Slowness (consensus is reached only on condition that each network node has completed the task – a smart contract or transaction verification. Due to the large number of nodes, the task processing time increases).

3) High cost (as the number of transactions increases, the cost of executing these transactions increases).

4) dentity data (anonymous participants can be intruders)

5) Immutability (although the immutability of transactions is an advantage of the public blockchain, it is at the same time its disadvantage. The blockchain considers a smart contract as a transaction. Any error inherent in the conditions of a smart contract cannot be corrected. Before creating a smart contract, programmable conditions must be carefully checked and tested before deployment).

6) Possibility of carrying out "51% attack"

7) Chance of centralization (to realize the benefits of public blockchains, standard nodes operate as full nodes. Full nodes are participants holding a complete copy of the blockchain. As the blockchain network grows in size, it becomes costly for small players and individual nodes to operate in only large players will be able to function as full nodes, which could lead to network centralization).

Public & closed blockchains, like open ones, are anonymous (pseudo-anonymous) immutable systems. Anyone can join the network by gaining access to read the available information, however, unlike open blockchains, the functions of confirming transactions lie with authorized users. Public Exclusive Shared Systems are intended for cases where certain people or authorities (for example, a designated employee or institution) confirm transactions that contain data that is available to the public for viewing. Public exclusive blockchains should not rely on such expensive consensus algorithms as Proof-of-Work, in the absence of the need to validate transactions by all network nodes. The most common consensus algorithm on an public & closed blockchain is Proof-of-Stake. The key feature of this algorithm is the absence of a mining process, and, accordingly, a large number of mathematical calculations that consume significant energy. People who confirm new transactions and create new blocks are called validators, and the process of confirming transactions is called *minting* (or *forging*). If in the Proof-of-Work algorithm the probability of successful mining depended on the presence of a large amount of computer power, then in Proof-of-Stake the cryptocurrency coin of this blockchain acts as the "weight" of the node's vote. Simply put, in order to become a validator, it is necessary to deposit a certain proportion of coins into the specified blockchain. Each holder of the cryptocurrency will receive interest for storage (analogous to a deposit in a bank) and will be able to confirm transactions. The higher the balance of the validator, the higher the probability of block generation. For example, Figure 6 shows four validators with token shares equal to 50, 30, 5 and 15%, respectively. Since validator № 1 has the most coins, he has a higher chance of signing a block than the rest. The determination of the user who signs the block is carried out according to the theory of probability, where the chance of signing the block is directly proportional to the number of coins deposited by the user.

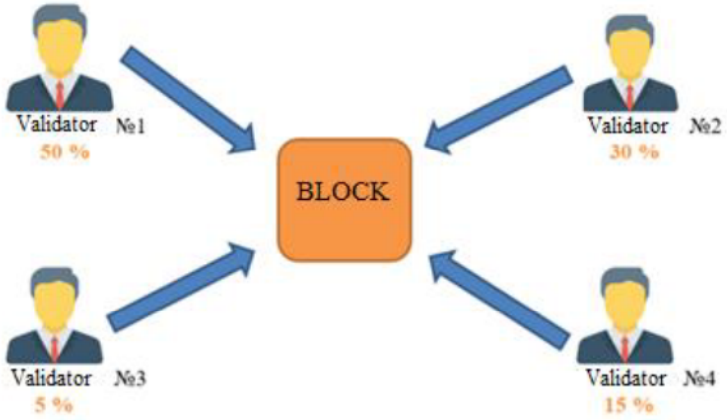

Fig. 6. The process of making consensus using the Proof-of-Stake algorithm

The Proof-of-stake algorithm is one of the most accessible types of consensus, that is, it has a low "entry threshold" due to the absence of the need to purchase expensive mining equipment. All you need for *forging* is a computer and a selected cryptocurrency. This algorithm solves the "environmental issue", which consists in increased energy consumption due to the most complex calculations. When using the consensus proof of ownership stake, the problem of the "arms race" inherent in the Proof-of-Work algorithm disappears, due to the direct dependence of the user's hash-

rate on the number of coins in the wallets of stakeholders, and not on computer power. It should be noted that the system is secure at the same time. So, to carry out a 51% attack, an attacker must acquire more than 50% of tokens and deposit them into the attacked blockchain. Thus, such attacks become financially impractical. As a result of an imbalance in the network and the stability of the attacked currency, the attacker will suffer himself.

The main disadvantage of the algorithm is the tendency towards centralization. Consensus encourages stakeholders to accumulate and retain funds on the balance sheet of the network, which contradicts the principles of decentralization originally laid down in the public blockchain.

Public exclusive blockchains retain the key advantages of open blockchains, such as the absence of the need for infrastructure costs to create and run decentralized applications (dApps), network transparency and immutability of transactions, and also solve the problem of low scalability by increasing the network bandwidth arising from the use of proof-of-stake consensus algorithm. However, such networks are less open and not fully decentralized. In addition, the disadvantages inherent in public open networks, such as immutability, the possibility of a 51% attack, identity and the chance of centralization, are also common to public & closed blockchains.

Conclusion. In conclusion, it should be noted the high importance of public blockchains in the modern world. A theoretical analysis of the existing literature shows that issues related to shared ledger technology have not been adequately studied. Thus, the results of this analysis allow us to draw conclusions that are of interest for research in the field of shared ledgers. First of all, the high importance of the proposed classification of blockchain systems into four categories is noted, each of which has a unique set of properties characteristic of a specific type of network. In the presented article, within the framework of a comprehensive classification, the category of public blockchains is separately distinguished. As a result of the analysis, the technical aspects of public shared ledgers are considered, where special attention is paid to consensus algorithms inherent in the category of public blockchains. In addition to technical aspects, the key advantages and disadvantages of such systems have been formed, which makes it possible to determine the possibilities of the practical use of shared ledger technology in various fields of activity. Thus, due to the transparency and immutability of the transactions made, the key properties of public blockchains, these categories find their application in the field of cryptocurrency circulation, electronic elections, copyright, as well as information management and audit.

However, the peculiarities of public blockchains impede the use of public shared networks in the field of commercial activities, and in particular in the field of transport and logistics services due to the need to provide free access to corporate information of the participating companies. In addition to confidentiality, public blockchains have scalability limitations that prevent the successful use of open ledgers in the freight and commercial space. To solve these problems, one should pay attention to closed blockchains, which are allocated as an element of further scientific research of shared ledger technology.

ЛИТЕРАТУРА

1. Попадюк А.Ю. Технические аспекты публичной распределенной сети на примере блокчейна Биткоин / А.Ю. Попадюк, Е.К. Коровяковский //Russian Journal of Logistics&Transport Management. 2019. с.116-125.

2. White Paper Bit Fury group «Public versus Private Blockchains» [Электронныйресурс]. Режим доступа:https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf свободный – (дата обращения: 27.01.2020).

3. О криптовалюте просто. Биткоин, эфириум, блокчейн, децентрализация, майнинг, ICO&Co. СПб.: Питер, 2019. 256 с.: (Серия «IT для бизнеса»)

4. Официальный сайт проекта *powercompare* [Электронный ресурс]. Режим доступа: https://powercompare.co.uk/bitcoin/свободный – (дата обращения: 27.01.2020).

REFERENCES

1. Popadyuk A.Yu. Tekhnicheskie aspekty publichnoj raspredelennoj seti na primere blokchejna Bitkoin / A.Yu. Popadyuk, E.K. Korovyakovskij //Russian Journal of Logistics&Transport Management. 2019. s.116-125.

2. White Paper Bit Fury group «Public versus Private Blockchains» [Elektronnyjresurs]. Rezhim dostupa:https://bitfury.com/content/downloads/public-vs-private-pt1-1.pdf svobodnyj – (data obrashcheniya: 27.01.2020).

3. O kriptovalyute prosto. Bitkoin, efirium, blokchejn, decentralizaciya, majning, ICO&Co. SPb.: Piter, 2019. 256 s.: (Seriya «IT dlya biznesa»)

4. Oficial'nyj sajt proekta powercompare [Elektronnyj resurs]. Rezhim dostupa: https://powercompare.co.uk/bitcoin/-svobodnyj – (data obrashcheniya: 27.01.2020).

ОБ АВТОРАХ | ABOUT AUTHORS

Попадюк А. Ю., Аспирант кафедры «логистика и коммерческая работа» Петербургского государственного университета путей сообщения Императора Александра I, дежурный по станции 1-го класса Апатиты, Апатиты, тел. (904) 2165103, e-mail: antonpopadyuk1997@yandex.ru

Popadyuk A. Yu., Postgraduate Student of the Logistics and Commercial Work Department, Emperor Alexander I St. Petersburg State Transport University, Apatity railway station master-on-duty, Apatity, ph. (904) 2165103, e-mail: antonpopadyuk1997@yandex.ru

Коровяковский Е. К., кандидат технических наук, доцент, и.о. заведующего кафедрой «логистика и коммерческая работа» Петербургского государственного университета путей сообщения Императора Александра I, Санкт-Петербург, e-mail: ekorsky@mail.ru

Korovyakovskiy E. K., Candidate of Technical Sciences, Associate Professor, Acting head of the Logistics

and Commercial Work Department, Emperor Alexander I St. Petersburg State Transport University,
e-mail: ekorsky@mail.ru

Дата поступления в редакцию: 03.04.2020
После рецензирования: 25.05.2020
Дата принятия к публикации: 31.05.2020