ORIGINAL PAPER

DOI: 10.26794/2587-5671-2020-24-5-84-99
UDC 336.012.23,336.018,336.711.2,336.741.2(045)
JEL A10, B53, E40, E42, E44

Institutional Features of the Development of Competitive Cryptocurrency

V.P. Bauer[a], **V.V. Smirnov**[b] ✉
Financial University, Moscow, Russia
[a] https://orcid.org/0000-0002-6612-3797; [b] http://orcid.org/0000-0003-0753-2520
✉ Corresponding author

ABSTRACT

The **aim** of the article is to clarify the basics of the digitalization strategy of the competitive businesses and identify features of the institutional environment that ensure the development of cryptocurrency as a new asset (IT product) of the modern economy, analyze the methods of implementing the cryptocurrency business models. The **relevance** of the research paper is determined by the need to develop a competitive Russian cryptocurrency (including the crypto-ruble) with the growing private, state and cross-national cryptocurrencies. The **scientific novelty** of the study implies clarifying the informal and formal rules of the institutional environment and related methods ensuring the development of a competitive cryptocurrency. The authors consider the following **methods** to implement the institutional features of the cryptocurrencies business model development: logic and blockchain algorithm that establish trust and collaboration between cryptocurrency developers; logic and blockchain consensus algorithm ensuring that all the parties of the blockchain network come to a common agreement (consensus); logic and blockchain algorithms that form cryptocurrency transactions and control its turnover by generating blocks of cryptocurrencies, by forming the structure of blocks and transactions of cryptocurrencies, by storing cryptocurrencies' keys and providing security, by mining (forging) cryptocurrency, etc. The **results** of the study provide a basis for identifying the institutional features and the corresponding methods providing a competitive cryptocurrency development with a detailed analysis of the blockchain consensus algorithms that ensure the competitiveness of the cryptocurrency. The **conclusions** show that the most promising are the hybrid consensus algorithms which may include both the logic of two or more known algorithms and the original logic of a new algorithm. The authors **recommend** defining the logic of the blockchain consensus algorithm as a priority when developing a cryptocurrency to ensure reliability of the transactions in the blockchain network, thus increasing the competitiveness of the cryptocurrency.

Keywords: institutional environment; formal and informal rules of the institutional environment; competition; cryptocurrency; business model; blockchain; logic; algorithm; consensus

For citation: **Bauer V.P., Smirnov V.V. Institutional features of the development of competitive cryptocurrency.** ***Finance: Theory and Practice.*** **2020;24(5):84-99. (In Russ.). DOI: 10.26794/2587-5671-2020-24-5-84-99**

INTRODUCTION

The first cryptocurrency Bitcoin started in 2009 on the basis of the blockchain algorithm developed by Satoshi Nakamoto [1], which implemented the thesis about the freedom of the creative person in the information society from the government intervention and its regulators [2]. This idea was introduced by cypherpunks[1] and crypto-anarchists in the 1990s last century [3, 4], but, as shown by P.I. Talerov [5], it is closely connected with the discussions of the 19th and 20th centuries about the importance of the market competition between anarchists and economists. Interestingly, the discussion resulted in a theory put forward by the Russian anarchist P.A. Kropotkin, which was accepted by the scientific community, that except for Darwinian competition, there is another fundamental law — mutual aid [6].

The development of digital financial assets changed the international world of finance [7] and triggered the onset of the era of cryptocurrencies [8]. The studies of the cryptocurrency features have identified them as a new financial asset [9].

With the massive emergence of private [10–12], state-run (Japan,[2] China,[3,4]) and shared (within the BRICS,[5,6]) cryptocurrencies and the active digital transformation of the Russian society[7] the issue of developing a Russian competitive cryptocurrency, for example, a crypto-ruble, is on the agenda [13, 14]. The analysis of the problem showed that it is necessary to identify the features of the institutional environment that form the cryptocurrency as a competitive asset of the digital economy and to determine the methods of their implementation in order to solve it.

COMPETITION AND COMPETITIVENESS OF IT PRODUCTS

The contemporary encyclopedia gives the following definition of competition: "... competition (from *Late Lat. concurentia, concurrere — to collide*), rivalry, a contest between people, groups, organizations for achieving similar goals, the best results in a particular social sphere. Competition is an essential feature of various types of activity where there is a clash of interests (politics, economics, science, sports, etc.)".[8]

In the monograph by E.V. Drobot it is noted that "... competition is one of the main characteristics of the market economy. The competition obliges a socially and legally free person to creative activity, creates conditions for personal fulfillment in the economic sphere in the form of developing new competitive goods and services" [15].

An integral part of the competition is the competitiveness of products, defined as "... the property of products to be attractive in comparison to other products of a similar type and purpose by better matching the requirements of a particular market and consumer evaluations. ... The characteristics of a product determine its consumer attributes, which, in turn, includes some quality indicators of this product. The competitiveness

[1] May T.C. The Crypto Anarchist Manifesto. Nov. 92. URL: https://www.activism.net/cypherpunk/crypto-anarchy.html (accessed on 15.05.2020).

[2] Cryptocurrency is recognized as a method of payment in Japan. URL: http://tass.ru/ekonomika/4144338 (accessed on 15.05.2020).

[3] Dorenkov I. Chinese authorities facilitate the launch of the digital yuan. URL: https://news.crypto.pro/vlasti-kitaja-forsirujut-zapusk-cifrovogo-juanja/ (accessed on 15.05.2020).

[4] Baloyan S. China launches state cryptocurrency: how it could change the financial world. URL: https://vc.ru/finance/122749-kitay-zapuskaet-gosudarstvennuyu-kriptovalyutu-kak-eto-mozhet-izmenit-finansovyy-mir (accessed on 15.05.2020).

[5] Goncharov A.I., Goncharova M.V. Digital Tokens in the Tools of Modern Foreign Trade Activities by Economic Entities of the BRICS Jurisdictions. Legal Concept. 2019;18(3):31–42. DOI: 10.15688/lc.jvolsu.2019.3.5

[6] Grigoryeva Y. BRICS Token: New Wave in International Payment System. URL: http://infobrics.org/post/30179/ (accessed on 15.05.2020).

[7] Digital Russia Report. Digital McKinsey. URL: https://www.mckinsey.com/ru/~/media/ McKinsey/Locations/Europe%20and%20Middle%20East/Russia/Our%20Insights/Digital%20Russia/Digital-Russia-report.ashx (accessed on 15.05.2020).

[8] Competition. Modern encyclopedia. URL: http://www.вокабула.рф/энциклопедии/современный-энциклопедический-словарь/конкуренция (accessed on 15.05.2020).

of a product depends both on a separate indicator and on their combination (synergy). The competitiveness of the product is ensured by the competitive positions occupied by the enterprises that produce and distribute the product. The indicators characterizing the competitiveness of the product <...> are a combination of "hard" and "soft" indicators <...>. "Hard" indicators provide the physical possibility of using goods for their intended purpose and are subdivided into the following groups: technical <...>, ergonomic <...>, technological <...>, and normative <...>. "Soft" indicators characterize the aesthetic <...> and psychological <...> characteristics of the product".[9]

Considering the definition of the competitiveness of products, the competitiveness of the cryptocurrency will be defined as follows.

Firstly, a competitive cryptocurrency should have a new consumer attribute that forms, in contrast to existing cryptocurrencies, its useful effect. As will be shown below, this attribute is ensured by the application of specific "hard" and "soft" rules of the institutional environment in which it was developed.

Secondly, a cryptocurrency should have characteristics that make it competitive among other cryptocurrencies. However, as shown in [16, 17], the market aspect of competitiveness of the cryptocurrency requires to study the rules for the functioning of the institutional environment of the crypto market as a whole, therefore, is not considered in this paper.

Research has shown that in practice two principles of developing competitive products may be used: systemic and process-based [18, 19]. In the first case, there is a competitive environment [20] that promotes product development. In the second case, the market-based [21] and inter-company processes [22] or inter-organizational structures [23, 24] are formed, contributing to the same process. Moreover, in the work of Yu. V. Taranukha showed that the development of economic relations in modern conditions leads to the evolution and modification of these principles [25].

The development of a competitive IT product was analyzed in the work of N. M. Rozanova and I. V. Lineva [26]. The authors argue that "... a competitive IT product is a modern business tool for transforming a traditional business model into a digital model". The authors note that "... an important aspect of the competitiveness of an IT product remains the same: what to produce and according to what formalized requirements?" Based on these assumptions, the authors summarize that "... a competitive IT product is a tool of modern business for transforming a traditional business model into a digital model", or, moreover, "... a competitive IT product is a digital model of a modern company using its key components: mobile devices, big data, cloud platforms".

To identify the rules (informal and formal) required to create such a competitive IT product as a cryptocurrency, we will consider the structure and composition of the institutional environment and methods that contribute to solving this problem.

RULES OF THE INSTITUTIONAL ENVIRONMENT, DEFINING PRACTICES AND DEVELOPMENT METHODS OF COMPETITIVE CRYPTOCURRENCY

There is a small bibliography on the institutional environment formation contributing to the development of competitive products. So, in the work of R. R. Nureeva and her colleagues [27], this issue is solely investigated at the macro level. In the work of I. A. Ivanenko and F. N. Saifidinova [28], the study of the institutional environment is associated with assessments of the instability of the economy arising in the competitive

[9] Competitiveness of products. Wikipedia. URL: https://ru.wikipedia.org/wiki/Конкурентоспособность_товара (accessed on 25.05.2020).

market environment. The most in-depth research on the formation of the institutional environment under competition is given in the monograph by A. Kh. Khakimov [29]. The author examines the influence of the institutional environment on the competitiveness management of enterprises in the context of the integration processes in the market. A. F. Grishkov in his work [30] substantiates that enterprises should develop and use software and hardware for dynamic monitoring and adjustment of competitiveness factors to manage competitiveness in a complex institutional environment.

The works by D. E. Sorokin [31, 32] show that the formation of the institutional environment of modern Russian society is significantly influenced not only by formal but also informal rules and practices. When developing cryptocurrencies, the significance of this idea is confirmed by the facts of using various rules and practices by venture entrepreneurs [33], representatives of different types of enterprises [34], and developers of digital platforms [35].

It was shown above that the characteristics of the competitiveness of any product are a set of "hard" and "soft" indicators. Let us define an appropriate set of "hard" and "soft" rules of the institutional environment and methods of their implementation.

In the study, we will proceed from the assumption that the "hard" indicators should ensure the physical possibility of using the product for its intended purpose. Then the "hard" rules of the institutional environment, first of all, should include technological solutions and regulatory requirements that contribute to the development of cryptocurrency as one of the types of IT products. In practice, these rules include strict logical methods for developing algorithms for business models of cryptocurrencies and standardized coding languages, on the basis of which the algorithms for these business models are developed. It should be noted that the issues of programming algorithms are not considered as the subject of this paper.

As for "soft" indicators of the competitiveness of cryptocurrencies, we include both psychological and ethical rules for the interaction of participants within the institutional environment, in which, on the one hand, cryptocurrency is created (cryptocurrency developers), and on the other hand, its circulation takes place (cryptocurrency users).

A competitive cryptocurrency should have a new consumer attribute that forms, in contrast to existing cryptocurrencies, its useful effect.

In the first case, approaches to the formation of a team that creates a cryptocurrency are of particular interest. The Agile flexible project management method for developing innovative products [36] and the associated programming methodology Scrum [37] have gained particular popularity. The aim of the Agile method is to use formal and informal relationship between developers' team members to create a competitive IT product in the shortest possible time, by using the Scrum methodology.

Within the framework of the Agile method, the institutional environment of cryptocurrency developers includes the following key elements: selecting participants and reaching an agreement on collaborative activities; agreeing on the team's mission; establishing boundaries of trust between participants; setting goals, objectives, and areas of interest; finding collaboration boundaries; highlighting key success factors and milestones; estimating resource; identifying the required skills for the development process, assessing them and, if necessary, adjusting the team members; review-

ing the results of the teamwork; disbanding the team.

Within the Scrum methodology, cryptocurrency development is implemented in practice by the following main methods:

- the logic and algorithm of the blockchain, establishing conditions of trust and collaboration in the innovative digital economy [38] between developers and users of cryptocurrencies [39, 40];
- the logic and algorithm of the blockchain consensus that solves the problem of the decentralized cryptocurrency turnover by reaching a compromise between transactions;[10]
- the logic and algorithms that form cryptocurrency transactions and protect their turnover, including the generation of cryptocurrency blocks, the formation of the structure of blocks and transactions, etc. [41];
- logic and algorithms of cryptographic protection and storage of cryptocurrency keys [42];
- the logic and algorithms of mining [43] (forging)[11] of cryptocurrencies, etc.

Studies of the market competitiveness of cryptocurrencies have shown that, firstly, the emission of cryptocurrencies is impossible without the processes of mining and forging [44]. Secondly, the logic of consensus algorithms plays a crucial role in transaction performance [45]. In this regard, we will consider this issue in more detail.

ANALYSIS OF THE CONSENSUS ALGORITHM LOGIC IN BLOCKCHAIN

The blockchain consensus algorithm is one of the key mechanisms in cryptocurrency development. Research by Russian patent experts has shown that at present in the international patent landscape, the consensus algorithm is included in almost all of the most cited patents protected in the field of cryptocurrencies. [46]. In general, a consensus is a mechanism for resolving conflicts within a group of participants involved in solving the problem of implementing transactions of a group of participants. A group of participants must side with each other and agree on a solution to the problem of completing the transaction. Blockchain does not implement the principles of distributed consensus, so they are implemented by third-party technologies that are usually used in distributed database systems, etc. The distributed consensus logic in the blockchain differs from the database consensus logic which is network-based. In database consensus, the number of nodes participating in a transaction is always known. In database consensus, blockchain nodes participating in a transaction may be dynamically selected. The behavior of participants in a network that implements distributed consensus is described as the Byzantine Generals Problem.[12] This problem was formulated by Lamport, Shostak, and Pease in 1982 last century [47], and a solution was found in the late 90s. The consensus algorithm includes a set of logical rules in the blockchain of a cryptocurrency, that determine who and under what conditions can confirm transactions, add new blocks, and perform other logical actions [48].

The logic of consensus algorithms ensures the adoption of an automated decision in the cryptosystem by implementing the following basic rules for the interaction of cryptocurrency users:

- agreement: reaching a common agreement of the interacting parties;
- egalitarianism: observance of equality, equal rights to every participant;

[10] Murzin P.E. Basic approaches to developing a consensus protocol in distributed ledgers. URL: https://www.granit-concern.ru/pdf/Murzin_statia_razrabotka_consensa_rr.pdf (accessed on 15.05.2020).

[11] What is forging? URL: https://bulldog.black/2019/04/27/chto-takoe-fordzhing-kriptovaljuty/ (accessed on 15.05.2020).

[12] Byzantine Generals Problem. URL: https://ru.wikipedia.org/wiki/Задача_византийских_генералов (accessed on 15.05.2020).

• cooperation: peers are interested in collaboration;
• inclusion: in the process of reaching agreement, there should be a maximum number of participants.

It should be noted that not only the decision-making process itself is called consensus, but also the decision itself, i.e. the result. Thus, in the blockchain, the consensus algorithm is a set of logically related rules and functions that automatically regulate the operation of the network of cryptocurrency users. Modern blockchain consensus algorithms are based on the logic of algorithms for solving the cryptographic Byzantine Generals Problem. However, the logic of the Byzantine problem was slightly changed and adapted for a P2P network to be used for cryptocurrencies. Considering the logic of this problem with regards to the blockchain, the following main features are distinguished:

Censorship resistance. The blockchain is a decentralized system that does not require a single governing body, hence, no one can prohibit mining to anyone, i.e. ensuring the operation of the network.

Objectivity. The blockchain contains relevant information describing the state of the network. Therefore, blockchain records do not need to be verified by any authoritative sources.

The functions of the blockchain consensus mechanisms are as follows:

The frequency of generating new blocks of records. These algorithms exclude situations each node generates its own block and the block that is added to the blockchain. For example, the Bitcoin network generates blocks every 10 minutes. However, sometimes there are situations when two or more nodes generate a block almost simultaneously, with a second apart. In this case, it leads to a conflict, which is resolved in favor of the node that created the block before everyone else. Transactions of the concurrent block or blocks are listed as invalid transactions and processed in the next block.

Verifying information of the record block. All participants need to confirm that the data in the generated block is correct. The hash transactions of the current and previous blocks are subject to verification, as well as the nonce number.

The amount of reward in the network. The size of the reward depends on the complexity of the network but, oddly enough, is inversely proportional to its complexity.

Preventing double-spending of funds (crypto coins). For example, in Bitcoin, when making a transaction, all funds are sent to the blockchain. After that, the required amount is transferred to the recipient, and the remainder is returned to the sender.

The main feature of the Nakamoto algorithm is that the more network participants, the greater the total computing power of the network, which means that to balance the cost of mined coins in time, it is necessary to increase the complexity of the calculations.

We consider the logic of the main consensus algorithms in the blockchain. ***Proof of Work (PoW)*** *— a proof-of-work algorithm of the network.* The logic of the algorithm determines that dedicated network nodes called “miners” must do the “work” to reach a distributed transaction agreement. The basic condition of the consensus algorithm is that the “work” must be guaranteed to be done. Which dedicated node spends less time on “work”, gets the right to close (commit) the transaction.

The Proof-of-Work concept was coined in 1993 but got its official term only in 1999. The works of Satoshi Nakamoto promoted

a massive application of the described algorithm. The main feature of the Nakamoto algorithm is that the more network participants, the greater the total computing power of the network, which means that to balance the cost of mined coins in time, it is necessary to increase the complexity of the calculations. This approach made it possible to unevenly distribute the number of mined coins over time. The number of mined coins decreases, the value of each mined coin increases.

To earn more crypto coins, miners increase the computing power of the equipment, which leads to a "race" effect. In the first implementation of the Nakamoto algorithm, a personal computer with a single processor was sufficient for mining bitcoins. Now computers need to be combined into farms, computer processors — into a processor pool, or large-capacity mining farms need to be built. Increasing the processing power of mining farms requires large amounts of electricity, which leads to increased global energy consumption due to the rapid obsolescence of computer technology.

Another shortcoming of the PoW algorithm is the low attack resistance of 51% of the involved computing power (computers). It is believed that such attacks are theoretical, however, it is known that for several hours the computing power of a large Russian industrial organization was transferred to the mining of one unpopular crypto coin. The mined coins were transferred to the crypto wallet of one of the organization's employees. Then a huge number of crypto-coins were promptly withdrawn to a crypto-exchange, exchanged for liquid crypto-currencies, sent to another crypto-exchange, and cashed there for fiat money.[13]

Proof of Stake (PoS) *— is an algorithm for proving the share of cryptocurrency ownership in the total cryptocurrency pool.* The PoS consensus algorithm ranks second in popularity due to its use in the implementation of cryptocurrencies. As a concept, the Proof of Stake algorithm was proposed in 2011 during the Bitcointalk forum,[14] and the first implementation of the protocol was introduced by the PeerCoin cryptocurrency[15] in 2012. The algorithm requires network participants — the owners of the cryptocurrency. They unite into groups and delegate their rights to mine coins to one participant, who forms a pool of participants for all their principals. Such a network is called a node.

Another option is also possible when a node is created by one network participant who has a large amount of cryptocurrency in his wallet. Such a participant offers to add other network participants to his node.

Activity management of the community of network participants, as well as the rules for managing consensus, is carried out only by the owners of the nodes, as the rights to this activity are delegated by other members of the network participants.

The node generates blocks in the network. The more coins a node has in a wallet, the more likely it is to generate a new block. Thus, a user who has up to 10% of all cryptocurrencies in a cryptocurrency wallet will be able to generate new blocks of the Blockchain network with an average probability of up to 10%.

In PoS algorithms, the entire amount of coins can be generated, and then these coins may be transferred between network participants. There are many ways to implement the PoS consensus algorithm, which are as follows:

[13] Smirnova E. Caught mining. Mining at work is punished. URL: https://www.forbes.ru/tehnologii/354613-pogoreli-na-kripte-kak-nakazyvayut-za-mayning-na-rabochem-meste (accessed on 15.05.2020).

[14] Cryptocurrencies Without Proof of Work. URL: https://link.springer.com/chapter/10.1007/978–3–662–53357–4_10 (accessed on 15.05.2020).

[15] PeerCoin website. URL: https://peercoin.net (accessed on 15.05.2020).

• Leased Proof of Stake (LPoS) — a leased-proof-of-stake algorithm. This is a pool of network participants with a small number of crypto coins, which they lease to participants with a large number of crypto coins, creating a node. By leasing crypto-coins, the network users get the opportunity to receive their share of the crypto-coins from the mining node, otherwise, the chance to receive a reward is low as the share of the network participant in the general cryptocurrency market is minimum.

• Delegated Proof of Stake (DPoS) — a delegated proof of stake of crypto coins. All network users select nodes to which they delegate the rights to generate new blocks. The selected network participants — node owners — decide on its development, as well as on the configuration of the cryptocurrency network.

PoW was the first algorithm, new algorithms were introduced to overcome its drawbacks. In PoS, cumbersome calculations are not required, which leads to reduced energy consumption and computing power. A 51% attack will also bring the greatest damage to the attacker as the purchase of such a quantity of cryptocurrency will lead to an increase in its value, which will require significant financial costs, therefore, the attack will make the attacker the main victim, because he will become the holder of most of the crypto tokens.

The process of mining cryptocurrency based on PoS consensus is called forging. It consists of setting up a masternode that runs on a dedicated computer, costing $ 70–100. The computer is always connected to the Internet. A crypto wallet with a minimum amount of cryptocurrency constantly runs on a dedicated computer. For example, a DASH node[16] requires 1,000 cryptocurrencies to run; for June 2020 at the exchange rate, this corresponds to $ 775,600. The operation of a masternode can only bring significant profits if transactions are carried out with unpopular cryptocurrencies that are not costly. If their value grows, the owner can increase their number and receive regular rewards on their masternode.

PoS disadvantages are:

• a user has to keep a large amount of coins in his wallet and cannot use them for purchases;

• PoS leads to inequality. The rich get richer, the poor get poorer. For example, a miner who owns 10% of a cryptocurrency receives 10% of all mined coins.

PoW and PoS consensus algorithms are constantly evolving and go in two directions, complicating their logic:

• a combination of algorithms is carried out in various ways. The PoS algorithm is used to generate new blocks, to confirm transactions (or vice versa);

• complication of the logic of the PoS algorithm to eliminate its shortcomings.

Proof of Importance (PoI) — *algorithm for proving the importance of a process*. Logically, the algorithm is similar to the PoS algorithm, but the following criteria are taken into account when generating a block:

• the amount of crypto tokens in the node's crypto wallet;

• network node lifetime;

• the number of successfully completed transactions by the network node.

This algorithm has the following peculiarity: the fewer crypto-coins there are in the node's own crypto wallet, the greater the influence of the number of transactions and the time the node is online on the result of the crypto-currency mining operation.

The logic of this algorithm is introduced, for example, in the NEM[17] cryptosystem, in which each account is assigned with an importance score. As the importance score increases, the account will have a better

[16] DASH website. URL: https://www.dash.org (accessed o 15.05.2020).

[17] NEM website. URL: https://nem.io/ru/ (accessed on 15.05.2020).

chance of receiving a cryptocurrency reward. In order to be eligible for importance calculation, users must hold at least 10,000 NEM crypto coins on the balance. How does the NEM network determine importance scores? If someone owns 10,000 NEM crypto coins or more, then a mathematical recalculation of transactions occurs. The increase in transactions on the network associated with this account will lead to an increase in the importance score. There is an opinion this threshold will be changed in the future. This method also ensures that users, NEM holders, will continue to save their funds. This method may be considered as the logic of creating a masternode. The project also provides visitors the ability to rank the importance of individual accounts on the network, which is a good way to keep the decentralized network going. The collection of rewards on the NEM blockchain is almost the same as in traditional mining. Its purpose is to add transactions to the blockchain in exchange for financial rewards.

Proof of Authority (PoA) *— a proof of authority algorithm*. Network participants give the right to create new blocks to the selected nodes. PoA can be applied to regulated and corporate cryptosystems. The PoA algorithm is not decentralized, all blocks are under the control of the developer. Therefore, it can be expected that it is the PoA algorithm that may be implemented in state cryptosystems.

Proof of Capacity (PoC) u Proof of Storage *— are algorithms for confirming the capacity of a computer's working memory*. This algorithm implies monetization of the allocated memory on the hard disk of the computer of a network participant. There are options to implement these algorithms to isolate the computing (processing) power of the computers of the network participants, which is also monetized.

Proof of Stake Time (PoST) *— a proof-of-stake algorithm is based on the age of the cryptocurrency*. In this case, instead of considering the number of cryptocurrencies, the period of time during which the cryptocurrencies were stored at a specific address is used to calculate their age. The algorithm is implemented in the VeriCoin cryptocurrency.[18]

Delegated Proof Of Stake (DPOS) *— an algorithm for delegating proof of ownership of a cryptocurrency*. DPOS uses EOS[19] and BitShares,[20] cryptocurrencies, while EOS uses consensus logic to scale the process to millions of transactions per second.

DPoS is different from Po S. In DPoS, stakeholders do not vote on the validity of the blocks but vote to elect delegates to do the validation on their behalf. There are between 21–100 elected delegates and they are shuffled periodically. The system is efficient. If the elected nodes continually miss their blocks or publish invalid transactions, stakeholders vote them out and replace them with a better delegate.

In DPoS, miners collaborate to make blocks which does not happen in PoW and Po S. Due to partial centralization in block creation, DPoS algorithm can work orders of magnitude faster than most other consensus algorithms.

TAPOS *— an algorithm in which a transaction is a proof of stake*. The algorithm is implemented in the software of the EOS crypto system. In this system, each transaction must contain a hash (reference) to the previous transaction. This ensures the following:

- preventing transaction reversal;
- generating a network signal indicating that the user and his share are in a certain fork;
- shaping a network signal that prevents validators from acting maliciously for purposes unforeseen by the logic of the process.

[18] VeriCoin website. URL: https://vericoin.info (accessed on 15.05.2020).
[19] EOS website. URL: https://eos.io (accessed on 15.05.2020).
[20] BitShares website. URL: https://bitshares.org (accessed on 15.05.2020).

BFT *— Byzantine Fault Tolerance (also Byzantine Generals Problem) algorithm*. It is implemented in Hyperledger,[21] Stellar,[22] Ripple[23] and other cryptocurrencies. The Federated Byzantine Agreement (FBA) is used with Stellar and Ripple cryptocurrencies. The idea is that each byzantine general, responsible for his own blockchain, sorts all messages in order to validate the truth. In Ripple, validator generals are pre-elected by the founders of Ripple. In Stellar, anyone can be a validator, therefore the user chooses which validators to trust. It is used for its high throughput, low transaction costs, and scalability. Currently, this algorithm is also actively used in Hyperledger Fabric. This provides high transaction throughput while fully centralizing the entire process.

dBFT *— a Delegated Byzantine Fault Tolerance* implemented in NEO.[24] The NEO creators have chosen this algorithm to provide better scalability and higher process performance. To explain the logic behind dBFT, we use the following simplified analogy. There is a country called NEO. Every citizen of a country has the right to vote when electing a leader, called a delegate. All the delegates form the laws of the country. If citizens disagree with how a delegate voted on the law, they can vote for another delegate. Then the citizens tell their elected ones what they want from them. Each delegate must keep track of the demands of all citizens and write them down in the book. These demands will be taken into account when passing laws aimed at ensuring that citizens are happy. When the time comes to pass a law, a speaker is randomly assigned from a group of delegates. He proposes a law based on the demands of citizens. In the proposed law, he explains how the law will affect a country's happiness number. The speaker will then personally present the proposed law to the delegates. Delegates decide whether the speaker's happiness level calculation matches their own. If 66% of delegates agree that the calculated number of happiness is correct, the law passes. If less than 66% of the delegates agree, a new speaker is selected randomly and the election process is repeated again. Thus, this algorithm is designed to protect citizens from traitors and leaders.

To ensure their competitiveness, cryptocurrency developers are advised to responsibly choose the consensus algorithm that forms rules aimed at solving the Byzantine Generals Problem of the cryptocurrency blockchain.

Applying this analogy to the NEO blockchain, anyone owning NEO is a citizen. The majority of NEO holders are Ordinary Nodes that can only transfer or exchange assets. Like citizens in the country of NEO, they do not participate in block validation. Delegates represent Bookkeeping Nodes in the NEO Economy. Bookkeeping Nodes verify each block written to the blockchain. To become a Bookkeeping Node certain requirements must be met, such as special equipment, dedicated internet connections, and a certain of amount of GAS[25] (1,000 at the time of writing). Then, the following logic is used: The law represents the current block in the blockchain and the Happiness Number is the hash of the current block.

The aBFT consensus algorithm is used in the Hashgraph cryptocurrency, in which nodes distribute their transactions random-

[21] Hyperledger website. URL: https://www.hyperledger.org/projects/fabric (accessed on 15.05.2020).

[22] Stellar website. URL: https://www.stellar.org (accessed on 15.05.2020).

[23] Ripple website. URL: https://ripple.com/xrp/ (accessed on 15.05.2020).

[24] NEO website. URL: https://neo.org (accessed on 15.05.2020).

[25] NEO website. URL: https://neo.org (accessed on 15.05.2020).

ly to other nodes. Therefore, transactions may "intertwine" around nodes. Hashgraph processes up to 250,000 transactions per second but it is not resistant to attacks like Sybil,[26] so it is only suitable for small private networks.

Proof Of Activity (PoA) — *a proof-of-activity algorithm* implemented in the Ethereum Kovan testnet.[27] This is a consensus algorithm, in which transactions are checked by dedicated "accountants", whose functions are similar to those of the system "admins". Other nodes learn about the state of the process from the "accountants". PoA has high bandwidth and is optimized for private networks. Obviously, due to the centralization of the process, PoA will not be able to function effectively in public networks.

Proof Of Burn — *coins burning algorithm* is implemented in Slimcoin.[28] The logic of the algorithm is that the miner has difficulties mining crypto-coins without attracting real resources, as in PoW algorithm with its power consumption costs and equipment. It also differs from PoS, in which it is necessary to accumulate cryptocurrencies.

By "burning" is meant the process of sending cryptocurrencies to an unspendable address (the details vary from cryptocurrency to cryptocurrency). Thus, the process script implies "deliberately silly" logic. But whoever donates crypto coins (similar to investing in mining) gets the right to charge a transaction fee. At the stage of earning a cryptocurrency, this is very useful for its market price.

Proof of Weight — *a proof-of-weight algorithm* is used in crypto systems Algorand,[29] Filecoin,[30] etc. This is a whole group of consensus algorithms. The general idea is that if in PoS, your percentage of tokens owned by the network gives you the likelihood of "finding" the next block, then PoWeight uses a different weighted value. Example: in the Filecoin Proof of Spacetime system, weighted by the number of IPFS cryptocurrencies in storage. Other systems may include conditions such as "proof of reputation".

Proof of Checkpoint — *an algorithm for checking matching blocks*. It is a hybrid algorithm that may use any PoS cryptocurrency system with a PoW algorithm. Each block used in one algorithm must find a similar block in another algorithm. The rhythm of the algorithm mitigates Proof of Stake attacks. However, hosts that are offline for an extended period of time are still vulnerable to these attacks. Disabled nodes when enabled can be used to provide false information about the blockchain.

Directed Acyclic Graphs (DAG) — *a directed acyclic graph algorithm*. DAG logic algorithms use Iota,[31] Hashgraph,[32] Raiblocks/Nano.[33] The DAG algorithm logic does not analyze the entire structure of the blockchain but processes its transactions asynchronously.[34] This makes it possible to process a significant number of transactions per second.

A specific example of a DAG-type consensus algorithm is Tangle,[35] used by Iota. In order to send a transaction, a user need to confirm two previously received transactions. Consensus logic, implemented on a two-for-one basis, enhances the validity

[26] Sybil attack. URL: https://ru.wikipedia.org/wiki/Атака Сивиллы (accessed on 15.05.2020).

[27] Ethereum Kovan website. URL: https://kovan.etherscan.io (accessed on 15.05.2020).

[28] Slimcoin website. URL: http://slimco.in (accessed on 15.05.2020).

[29] Algorand website. URL: https://www.algorand.com (accessed on 15.05.2020).

[30] Filecoin website. URL: https://filecoin.io (accessed on 15.05.2020).

[31] Iota website. URL: https://www.iota.org (accessed on 15.05.2020).

[32] Hashgraph website. URL: https://www.hedera.com (accessed on 15.05.2020).

[33] Nano website. URL: https://nano.org/en (accessed on 15.05.2020).

[34] Sompolinsky Y., Zohar A.A Scalable BlockDAG protocol. 2018. URL: http://diyhpl.us/~bryan/papers2/ bitcoin/Phantom:%20A%20scalable%20block%20DAG%20protocol%20-%202018.pdf (accessed on 15.05.2020).

[35] Popov S. The tangle. 2018. URL: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf (accessed on 15.05.2020).

of transactions. Since the consensus is established by the transactions, in theory, if someone can generate one third of all the transactions, they can take over the entire network. Therefore, Iota is "double-checking" of all network's transactions on a centralized "coordinator" node, which first functions to keep the system running, and then, when the number of processed nodes becomes very large, is removed.

CONCLUSIONS

The research results showed that the institutional features of the development of a competitive cryptocurrency were influenced not only by the development of information technologies, but also by the development of philosophy, mathematics, economics and finance. Analysis of "soft" and "hard" competition rules, institutional environment and methods that ensure the development of cryptocurrency shows that thanks to the efforts of many scientists and practicing programmers from around the world, cryptocurrency has become a new competitive asset (IT product) of modern finance.

The paper discusses in detail one of the "hard" rules of competition — the logic of blockchain consensus algorithms, which makes one of the main contributions to ensuring the competitiveness of cryptocurrencies. The analysis of the consensus logic is carried out for a limited number of algorithms that exist or are being tested. It has been shown that historically the first consensus algorithm was PoW, which is implemented in many cryptocurrencies of the Top 10 cryptocurrency list. Thus, in practice, this particular algorithm is the most common among cryptocurrency developers. However, its competitor (PoS algorithm) is already gaining its share of the cryptocurrency market, therefore, for example, Ethereum is switching to this algorithm. Research has revealed that the most promising are hybrid algorithms. They either combine the logic of PoS and PoW algorithms or are the results of the development and refinement of one of them (most often PoS logic).

Based on the results of the study, the following conclusions can be drawn.

Firstly, all consensus algorithms implement certain logical dependencies, and they have both strengths and weaknesses, so you need to be a professional mathematician to analyze this logic in detail. Most often, the differences in the names of the blockchain consensus algorithms emphasize the specifics of the logic: Work, Stake, Authority, Storage, etc.

Secondly, the logics of the development of blockchain consensus algorithms presented in the study are applicable to almost all cryptocurrencies, therefore, they are defined as the main ones:

- agreement;
- egalitarianism (business model of a specific cryptocurrency or cryptosystem determine the specifics of its implementation);
- cooperation;
- inclusion (it determines the algorithm "hacking" resistance, which may change under different conditions, therefore, only applied mathematicians can find inclusion specifics);
- censorship resistance;
- objectivity;
- frequency of generating new blocks of records (depends on the implementation technology of consensus algorithms, which have no such limits, as a rule);
- verification of information in the block of records (depends on the implementation technology of consensus algorithms, however, many methods of the verification may be implemented for the same algorithm);
- reward amount in the network (determined by the developer's view on its amount when implementing a specific consensus algorithm for a specific cryptocurrency);
- preventing double-spending of cryptocurrency (the procedure is mandatory for

the implementation of business models for all types of cryptocurrencies — the logic of the procedure provides a transaction that functions in parallel with the implementation of the main algorithm).

Thirdly, each cryptocurrency has unique characteristics, the analysis of which makes it possible to compare the effectiveness of the implementation of their business models to assess competitiveness. The practice has shown that the same business model can be implemented in several ways and based on different consensus algorithms. Therefore, it is possible to compare the competitiveness of the logic of consensus algorithms only after they are applied in the business models of specific cryptocurrencies, which will reveal their competitiveness in the crypto markets.

Thus, to ensure their competitiveness, cryptocurrency developers are advised to responsibly choose the consensus algorithm that forms rules aimed at solving the Byzantine Generals Problem of the cryptocurrency blockchain. These rules provide transactions with the information they use to reach consensus, keeping the network secure, and eliminating connection hang-ups. However, it should be emphasized that the conclusion about the competitiveness of a particular cryptocurrency can only be ensured by practicing in the crypto market

REFERENCES

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. URL: https://bitcoin.org/bitcoin.pdf (accessed on 15.05.2020).
2. Isaacson W. The innovators: How a group of hackers, geniuses, and geeks created the digital revolution. New York: Simon & Schuster; 2014. 560 p. (Russ. ed.: Isaacson W. Innovatory. Kak neskol'ko geniev, khakerov i gikov sovershili tsifrovuyu revolyutsiyu. Moscow: Mann, Ivanov and Ferber; 2019. 304 p.)
3. Ludlow P. High noon on the electronic frontier: Conceptual issues in cyberspace. Cambridge, MA: The MIT Press; 1996. 558 p.
4. Ludlow P. Crypto anarchy, cyberstates and pirate Utopias. Cambridge, MA: The MIT Press; 2001. 451 p.
5. Talerov P.I. Competition as a social phenomenon and the attitude of anarchists towards it. In: Proc. All-Russ. conf. with int. particip. "Interdisciplinary synthesis of the humanities in the era of sociocultural and historical transformations: Experience of the "Russian Way". St. Petersburg: Russian Christian Humanitarian Academy; 2019:113–120. (In Russ.).
6. Kropotkin P.A. Ethics. Selected works. Moscow: Politizdat; 1991. 496 p. (In Russ.).
7. Maslennikov V.V., Fedotova M.A., Sorokin A.N. New financial technologies are changing our world. *Vestnik Finansovogo universiteta = Bulletin of the Financial University*. 2017;21(2):6–11. (In Russ.). DOI: 10.26794/2587–5671–2017–21–2–6–6–11
8. Polanski A. The era of cryptocurrency. Moscow: AST; 2018. 320 p. (In Russ.).
9. Stolbov M.I. To the tenth anniversary of the cryptocurrency market: Current state and prospects. *Voprosy ekonomiki*. 2019;(5):136–148. (In Russ.). DOI: 10.32609/0042–8736–2019–5–136–148
10. Vigna P., Casey M.J. The age of cryptocurrency: How bitcoin and the blockchain are challenging the global economic order. London: Picador; 2016. 384 p. (Russ. ed.: Vigna P., Casey M. Epokha kriptovalyut. Kak bitkoin i blokcheyn menyayut mirovoy ekonomicheskiy poryadok. Moscow: Mann, Ivanov and Ferber; 2017. 432 p.).
11. Bauer V.P., Smirnov V.V. Bitcoin: Genesis, practice and development prospects. Part 1. *Informatsionnoe obshchestvo = Information Society*. 2018;(4–5):65–75. (In Russ.).
12. Bauer V.P., Smirnov V.V. Bitcoin: Genesis, practice, and development prospects. Part 2. *Informatsionnoe obshchestvo. = Information Society*. 2019;(1–2):35–43. (In Russ.).
13. Nedosekin A.O., Reishakhrit E.I, Abdulaeva Z.I. Russian crypto ruble — a tool for sustainable development of the Russian economy. *Ekonomika i predprinimatel'stvo = Journal of Economy and Entrepreneurship*. 2017;(9–1):65–71. (In Russ.).

14. Glaz'ev S. Yu. On the root causes of the growing chaos and measures to overcome the economic crisis. 2020. URL: https://glazev.ru/articles/1-mirovoy-krizis/78041-o-glubinnykh-prichinakh-narastajushhego-khaosa-i-merakh-po-preodoleniju-jekonomicheskogo-krizisa (accessed on 15.05.2020). (In Russ.).
15. Drobot E. V. Management of the competitiveness of the national economy in the context of globalization. St. Petersburg: Troitskii most; 2015. 223 p. (In Russ.).
16. Bauer V. P., Smirnov V. V. Comparative analysis of NEO and ETHEREUM cryptocurrencies in the context of the formation of the digital economy of the future. *Ekonomika. Nalogi. Pravo = Economics, Taxes & Law*. 2019;12(3):116–124. (In Russ.). DOI: 10.26794/1999–849X-2019–12–3–116–124
17. Sinel'nikova-Muryleva E.V., Shilov K. D., Zubarev A. V. The essence of cryptocurrencies: Descriptive and comparative analysis. *Finansy: teoriya i praktika = Finance: Theory and Practice*. 2019;23(6):36–49. (In Russ.). DOI: 10.26794/2587–5671–2019–23–6–36–49
18. Taranukha Yu. V. Competition. System and process. Moscow: Delo i servis; 2012. 665 p. (In Russ.).
19. Oskirko A. L. Methodology for assessing the status of the process of managing the competitiveness of goods (services) of an organization. *Colloquium-Journal*. 2019;(6–11):79–81. (In Russ.).
20. Bain E. E., Vorob'eva L. G. Theoretical aspects of the definition of the concept "competitive environment in the industry". *European Science*. 2017;(4):43–47. (In Russ.).
21. Biksina N. A. Competition in business: A complete definition of the concept, types, pros and cons of competition. *Ekonomika i upravlenie: problemy, resheniya.* 2018;2(5):4–7. (In Russ.).
22. Khakimov A. Kh. Competitive partnership of business organizations. *Zhurnal pravovykh i ekonomicheskikh issledovanii = Journal of Legal and Economic Studies*. 2019;(3):200–205. (In Russ.). DOI: 10.26163/GIEF.69.99.034
23. Kataev A. V., Kataeva T. M. Interorganizational network structures: Problems of organization and management. *Konkurentosposobnost' v global'nom mire: ekonomika, nauka, tekhnologii = Competitiveness in the Global World: Economics, Science, Technology*. 2016(7–1):141–144. (In Russ.).
24. Chi M., Zhao J., George J. F., Li Y., Zhai S. The influence of inter-firm IT governance strategies on relational performance: The moderation effect of information technology ambidexterity. *International Journal of Information Management*. 2017;37(2):43–53. DOI: 10.1016/j.ijinfomgt.2016.11.007
25. Taranukha Yu. V. Modification of the competitive principle in the evolution of competition. *Obshchestvo i ekonomika = Society and Economy*. 2017;(3–4):49–67. (In Russ.).
26. Rozanova N. M., Lineva I. V. Digital model for modern business. *Zhurnal ekonomicheskoi teorii = Russian Journal of the Economic Theory.* 2019;16(1):46–59. (In Russ.). DOI: 10.31063/2073–6517/2019.16–1.5
27. Nureeva R. R., Sharafutdinov R. I., Safiullin L. N. Digital competitiveness: Institutional foundations of the competitiveness of the Russian Federation in the digital economy. *Ekonomika i predprinimatel'stvo = Journal of Economy and Entrepreneurship*. 2018;(9):91–95. (In Russ.).
28. Ivanenko I. A., Saifidinova F. N. Institutional environment and competitive relations in the market. *Ekonomika i sotsium*. 2017;(12):455–457. (In Russ.).
29. Khakimov A. Kh. Problems of managing the competitiveness of Russian business structures and ways to solve them. St. Petersburg: St. Petersburg State University of Economics; 2019. 200 p. (In Russ.).
30. Grishkov A. F. A comprehensive model of the competitiveness management mechanism in the service sector. *Peterburgskii ekonomicheskii zhurnal = Saint-Petersburg Economic Journal*. 2019;(2):121–133. (In Russ.).
31. Sorokin D. E. On Russia's ability to social and economic transformations. *Ekonomicheskoe vozrozhdenie Rossii = The Economic Revival of Russia*. 2019;(1):23–28. (In Russ.).
32. Sorokin D. E. Political economy of technological modernization of Russia. *Ekonomicheskoe vozrozhdenie Rossii. = The Economic Revival of Russia*. 2020;(1):18–25. (In Russ.).

33. Romans A. The entrepreneurial Bible to venture capital: Inside secrets from the leaders in the startup game. New York: McGraw-Hill Education; 2013. 256 p. (Russ. ed.: Romans A. Nastol'naya kniga venchurnogo predprinimatelya. Sekrety liderov startapov. Moscow: Alpina Publisher; 2015. 246 p.).
34. Marakhovskaya I. Yu. The development of entrepreneurial structures in the face of increasing competitive challenges and threats. *Uchenye zapiski Krymskogo federal'nogo universiteta im. V. I. Vernadskogo. Ekonomika i upravlenie = Scientific Notes of V. I. Vernadsky Crimean Federal University. Economics and Management.* 2018;4(1):79–83. (In Russ.).
35. Eferin Ya. Yu., Rossotto K. M., Khokhlov Yu. E. Digital platforms in Russia: Competition between national and foreign multilateral platforms stimulates economic growth and innovation. *Informatsionnoe obshchestvo = Information Society*. 2019;(1–2):16–34. (In Russ.).
36. Stellman E., Greene J. Learning Agile: Understanding Scrum, XP, Lean, and Kanban. Sebastopol, CA: O'Reilly Media; 2013. 420 p. (Russ. ed.: Stellman E., Greene J. Postigaya Agile: Tsennosti, printsipy, metodologii. Moscow: Mann, Ivanov and Ferber; 2017. 445 p.).
37. Sutherland J. Scrum: The art of doing twice the work in half the time. New York: Crown Business; 2014. 256 p. (Russ. ed.: Sutherland J. Scrum. Revolyutsionnyy metod upravleniya proektami. Moscow: Mann, Ivanov and Ferber; 2017. 272 p.).
38. Nosova S. S. Strategy for an innovative economy in collaboration mode. *Ekonomicheskie strategii = Economic Strategies*. 2018;20(6):48–57. (In Russ.).
39. Bauer V. P., Pobyvaev S. A., Sil'vestrov S. N. Blockchain as an augmented reality: From a hypothesis to the basics of theory and practice. *Ekonomicheskaya nauka sovremennoi Rossii = Economics of Contemporary Russia*. 2018;(1):20–32. (In Russ.).
40. Krylov G. O., Seleznev V. M. Status and prospects of development of blockchain technology in the financial sector. *Finansy: teoriya i praktika = Finance: Theory and Practice*. 2019;23(6):26–35. (In Russ.). DOI: 10.26794/2587–5671–2019–23–6–26–35
41. Urakhchinsky I. N., Kondratiev S. V., Khayrislamov D. A., Koshmin M. D. Comparative analysis of encryption algorithms in the "Blockchain" technology. Coll. selected pap. of the Humanitarian National Research Institute "Natsrazvitie" sci. conf. St. Petersburg: HNRI "Natsrazvitie"; 2019:130–134. (In Russ.).
42. Mayorova E. V. Methodological aspects of responding to information security incidents in the digital economy. *Peterburgskii ekonomicheskii zhurnal = Saint-Petersburg Economic Journal*. 2020;(1):155–162. (In Russ.). DOI: 10.25631/PEJ.2020.1.155.162
43. Ershova I. V., Trofimova E. V. Mining and business activities: In search of balance. *Aktual'nye problemy rossiiskogo prava = Actual Problems of Russian Law*. 2019;(6):73–82. (In Russ.). DOI: 10.17803/1994–1471.2019.103.6.073–082
44. Urakhchinsky I. N., Khayrislamov D. A., Kondratiev S. V., Koshmin M. D. Comparative analysis of mining algorithms in the "Blockchain" technology. Coll. selected pap. of the Humanitarian National Research Institute "Natsrazvitie" sci. conf. St. Petersburg: HNRI "Natsrazvitie"; 2019:134–138. (In Russ.).
45. Kruteeva O. V., Solovieva Yu. Yu. A model for evaluating the effectiveness of cryptocurrency mining. *Ekonomika i predprinimatel'stvo = Journal of Economy and Entrepreneurship*. 2018;(11):1190–1193. (In Russ.).
46. Demin V. I., Solov'ev P. S., Trifonov M. I. et al. Blockchain technologies: Current status and key insights. Moscow: Federal Institute of Industrial Property; 2018. 87 p. (In Russ.).
47. Merkle R. C. Protocols for Public Key Cryptosystems. In: IEEE Symp. on security and privacy (Oakland, CA, 14–16 Apr. 1980). New York: IEEE; 1980:122. DOI: 10.1109/SP.1980.10006
48. Dolzhik D. S. Review and comparison of algorithms for finding consensus in the blockchain. In: Proc. 13th Int. sect. sci.-tech. conf. "Technology of the information society". Moscow: Media Publisher; 2019:349–351. (In Russ.).

ABOUT THE AUTHORS

Vladimir P. Bauer — Dr. Sci. (Econ.), Assoc. Prof., Head of the Centre of Strategic Forecasting and Planning, Institute for Economic Policy and Problems of Economic Security, Moscow, Russia
bvp09@mail.ru

Vladimir V. Smirnov — Junior Researcher of the Centre of Strategic Forecasting and Planning, Institute for Economic Policy and Problems of Economic Security, Moscow, Russia
Vladimir.Smirnov.fsg@gmail.com

The article was submitted on 08.06.2020; revised on 20.06.2020 and accepted for publication on 12.08.2020.
The authors read and approved the final version of the manuscript.