ORIGINAL PAPER

DOI: 10.26794/2587-5671-2019-23-6-36-49
UDC 336.012.23,336.018,336.711.2,336.741.2(045)
JEL A10, B53, E40, E42, E44

The Essence of Cryptocurrencies: Descriptive and Comparative Analysis

E.V. Sinel'nikova-Muryleva[a], **K.D. Shilov**[b], **A.V. Zubarev**[c]
Institute of Applied Economic Research, RANEPA, Moscow, Russia
[a] https://orcid.org/0000-0001-7494-2728; [b] https://orcid.org/0000-0002-2149-3946;
[c] https://orcid.org/0000-0003-2945-5271

ABSTRACT

The aim of the article is to systematize the views on the concept of cryptocurrency from the literature and among international and national organizations and regulators, to analyze its economic essence and the place in the modern monetary and financial system. The definition and the functions of cryptocurrency are discussed in the framework of descriptive and theoretical analysis. The paper systematized the existing approaches to the concept analysis of cryptocurrency; the place of cryptocurrency in modern economic theory is shown.The article concludes that cryptocurrencies are often determined through the set of basic characteristics. Cryptocurrencies are not money, though they can perform the main function of money — to be a means of payment; they can be a means of making settlements, assets, platforms for concluding smart contracts, a means for crowdfunding. They are not private money in Hayek's interpretation. Cryptocurrencies can be described in the framework of the models of new monetarism (payment economics).

Keywords: cryptocurrencies; crypto assets; payment systems; private money; economics of payments; blockchain

For citation: **Sinel'nikova-Muryleva E.V., Shilov K.D., Zubarev A.V. The essence of cryptocurrencies: descriptive and comparative analysis. *Finance: Theory and Practice.* 2019;23(6):36-49. DOI: 10.26794/2587-5671-2019-23-6-36-49**

INTRODUCTION

Amid its rapidly increasing and immense professional and public interest the subject of cryptocurrencies has raised the number of studies. The analysis of the economic nature of cryptocurrencies and their functions are widely discussed.

Cryptocurrencies and distributed ledger technology are two key concepts related to cryptoeconomics. The distributed ledger technology (blockchain) is often considered separately from cryptocurrencies, since it is only a certain type of database, the basis for cryptocurrencies. During the cryptocurrency boom, many large enterprises and even states were experimenting with distributed ledgers and were trying to apply them in various sectors of the economy. However, a significant part of these projects remained ink on paper or their implementation was limited to pilot launches and tests. At the same time, some experiments were successful, and today blockchain is used in information systems of government, medicine, and logistics. Nevertheless, experience has shown that blockchain without cryptocurrencies is a rather specific product that can show all its benefits compared to classical databases only under certain conditions.

As for cryptocurrencies, Bitcoin is mostly discussed in the academic community, although by now, the popularity of other cryptocurrencies has also grown significantly. Modern cryptocurrencies differ from each other not only by the features of the cryptographic algorithms, by the mechanisms of consensus, by the issuance and the degree of (de)centralization, but also by their target functions. Besides, many cryptocurrencies are considered as a potential investment tool. This work follows the previous research and aims to systematize the views on cryptocurrencies and their essence that exist in the literature.

BLOCKCHAIN AS THE BASE FO CRYPTOCURRENCIES

Most cryptocurrencies run on blockchain technology, which is a type of a distributed ledger, i.e. represents a certain type of database. Each block in blockchain contains a set of transactions completed during a certain period of time.

There are several classifications of blockchain by various criteria. In the light of the discussion about cryptocurrencies, the method of forming a blockchain (adding new blocks) is of interest. It is determined by the type of consensus, i.e. the mechanism, which decides on the degree of information security and how new blocks of information are formed.

There are three main types of consensus mechanism algorithms: "proof-of-work", "proof-of-stake" and "proof-of-authority", the algorithm based on solving the Byzantine Generals' Problem (it has not proved its effectiveness).

Before we speak more specifically about the types of consensus, it is necessary to define another term important for blockchain — "a node".

A node is a device in a blockchain network, i.e. any electronic device, such as a computer or telephone that has an Internet connection and an IP address. Nodes maintain the network by saving a copy of blockchain and, in some cases, processing transactions. Owners of nodes provide their computing resources to store and verify transactions, so they may get a transaction fee (commission). This is called mining (mining for PoW algorithms) or forging (forging for PoS algorithms).

There are two types of nodes:

1. A full node downloads the entire data of a specific blockchain and validates any new transaction, thus confirming and conducting transactions, placing them in blocks.

2. A partial (or lightweight) node does not store complete ledger. Thus, blockchain size is not a problem for this type of nodes, since there is no need to store a huge amount of data. Lightweight nodes only download the part of the blockchain which they require using SPV (Simplified Payment Verification) mode. They will connect to full nodes clients and use bloom filters to ensure that they only receive transactions, which are necessary and relevant to their operations.

The proof-of-work (PoW) is a common consensus algorithm used by the most popular cryptocurrency network Bitcoin. The idea is that the nodes of the blockchain compete to start the generation of each new block, which is called mining. The competition consists in solving a cryptographic problem (select a particular hash[1] of a certain complexity, which will serve as the header of a new block). This is what determines the competitive nature of mining: the more computing power is added to the network, the higher average number of calculations needed to create a new block. This method also increases the cost of the block creation, increasing the efficiency of the system. As a reward for its work, the victorious miner gets some new Bitcoin. This reward for recording a new block (solving a cryptographic problem) represents the currency issue. The Bitcoin protocol, as well as many other cryptocurrencies, is designed in such a way that issuance occurs at approximately equal intervals of time, and the value of each issuance is known in advance and is defined in the protocol properties; therefore, the trajectory of all future issuances, and therefore the cryptocurrency supply path, is known in advance.

The PoW enables any Bitcoin user to make secure transactions without the intervention of third parties. However, the main blockchain's weaknesses that form the very essence of currencies such as Bitcoin are well known. They consist in low transaction speed, fluctuating, and sometimes, high transaction costs. In addition, mining operations to verify blockchain process are associated with huge energy consumption.

The "proof-of-stake" consensus algorithm determines the probability of a participant to

[1] A hash is the result of a hash function. Such functions help prevent rewriting any information, since in this case it will be necessary to rewrite all subsequent blocks, which is impossible (see [1] for more details).

create a new block by the number of cryptocurrencies / tokens on their balance. The main PoS advantage is that there is no need to spend a large amount of energy on cryptographic problems. At the same time, while a new block is created, no more cryptocurrency is produced — the only reward is the fee from the transactions included in the block.

It is also possible to combine PoW and PoS mechanisms when some of the blocks are mined (for example, every n^{th} block, i.e. the place of such blocks in the chain is determined, the remaining blocks are added by validators).

The idea of the consensus mechanism based on solving the Byzantine Generals' Problem (byzantine fault tolerance algorithms, BFTA) is the constant exchange and reconciliation of ledger copies between the network participants resulting in consensus. Such systems are characterized by high transaction speed and lack of mining. The nodes participating in the consensus (depending on the cryptocurrency) can get some transaction fees from approved transactions. Such algorithms demonstrate high transaction speed with only a relatively small number of decision nodes and, therefore, are more often used in partially centralized ledgers.

Depending on the issuing mechanism, the vast majority of cryptocurrencies can be divided into those with limited offer, and the maximum amount is delayed, and those whose offer is fully issued at the moment when cryptocurrency is created.

Cryptocurrencies of the first type usually use PoW as a consensus mechanism, when the generation of new coins is a reward to miners, network participants, creating new blocks in the chain by using their computing power (Bitcoin, Etherium).

Cryptocurrencies of the second type use other consensus mechanisms, for example, PoS, where the likelihood of becoming a participant in creating a new block depends on the balance of coins in the account, the computational work is not so expensive, and the reward is only the fee from approved transactions (Nxt, BlackCoin).

Most common is using both consensus mechanisms[2], when most of the blocks are created by PoS, but some "holding" blocks are created by mining (EmerCoin, PeerCoin).

There are other methods of consensus and issuance. For example, in the Stellar decentralized platform for currency transactions, with its own lumen currency, the consensus mechanism is based on a particular solution to the Byzantine Generals' Problem (Federated Byzantine Agreement, FBA) [2]. Stellar had 100 billion lumens created at the genesis of the project, most of which are still not in free circulation (belong to the founders). Nevertheless, the following so-called inflationary mechanism was installed in the system, ensuring an increase of coins at a rate of 1% per year. Stellar charges a fee for each transaction. The fee pool is the lot of lumens collected from transaction fees. The pool plus the number of coins in circulation, multiplied by the coefficient of weekly inflation, is distributed to a certain number of network participants. They are chosen by other participants' votes — everyone can vote once for someone else; the vote is weighted by the number of lumens on the balance. Anyone who gains more than 0.05% of the total number of votes (i.e., from the total number of coins) is rewarded from the weekly fee pool.

Again, three main consensus mechanisms used to create cryptocurrencies today are proof-of-work, proof-of-stake and proof-of-authority (the algorithm based on solving the Byzantine Generals' Problem). Each of them has its flaws and weaknesses. For example, a not-so-popular cryptocurrency based on PoW can be attacked by temporary rental of huge computing power (which has been done several times and is called "51% attack").

Cryptocurrencies based on PoS are potentially vulnerable to other types of attacks, such as "deep attacks". If someone gains control over wallets containing already spent coins, s/he will be able to "roll back" the time until the mo-

[2] Note, that two most common and well-known cryptocurrencies — Bitcoin and Ether — use the non-hybrid consensus mechanism.

ment when these wallets contained coins, and, having thus obtained 51% of the coins, build an alternative blockchain. If this new alternative blockchain is longer than the main one, the attacker will change the contents of the blockchain backdated. Additional mechanisms, for example, dynamic checkpoints, are used to protect against such attacks. Overall, PoS turned out to be more stable than Po W. Nevertheless, it is now quite common to use both consensus mechanisms for issuing cryptocurrencies, since it reduces the overall risk of cyber-attacks.

DEFINITIONS OF CRYPTOCURRENCY AND ITS FUNCTIONS

There is no single definition of cryptocurrency. For example, the Bank for International Settlements (BIS) equates the concepts of "virtual currency"[3], "digital currency" and "cryptocurrency"[4] and defines "digital currency" based on the following key characteristics:

- issued only electronically;
- is not issued in national currencies and is not related to them;
- is no one's obligation (unlike traditional money);
- has zero intrinsic value, i.e. does not generate a stream of payments;
- is used for peer-to-peer exchange, i.e. direct (decentralized) exchange between the parties in the system using distributed ledger technology;
- is an asset with some characteristics of money (in particular, it is a means of payment).

Thus, the BIS interprets cryptocurrency as an asset with a number of unique characteristics. It is noteworthy that the BIS calls digital currencies potential substitutes for electronic money. Traditionally, the concept of money is defined through its functions[5]. In particular, according to the ECB report[6], "money is anything that is used widely to exchange value in transactions. It functions as a medium of exchange, storage of value and unit of account". Banknotes and coins are usually just a small part of the country's total money supply. According to the UK Financial Conduct Authority[7], electronic money (e-money) is electronically (including magnetically) stored monetary value, represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions. It must be accepted as a means of payment by a person other than the electronic money issuer. Types of e-money include pre-paid cards and electronic pre-paid accounts for online use

The ECB defines electronic money (e-money) as "an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer. The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions"[8]. As a rule, electronic money is stored in the same account as the fiat money used to create electronic money. It is different for cryptocurrencies.

The ECB refers to cryptocurrencies as to "decentralized, bi-directional virtual currency schemes"[9]. The term "virtual currency" is defined as a digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money. The term "virtual currency scheme(s)" is used

[3] Definition in ECB report (see European Central Bank. Virtual currency schemes. ECB Report. 1–55, October 2012): "A virtual currency is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community".

[4] See Bank of international settlements, CPMI. *Digital currencies.* 2015; Bank of international settlements, CPMI. *Central bank digital currencies.* 2018.

[5] Note, that in work [3], one of the earliest studies of the theoretical direction of the new monetarism and the economics of payments, money is identified with "memory" about the good behavior of an economic agent in the past: if "today" a person has money, it means "yesterday" they made their goods delivery commitments to the counterparty.

[6] European Central Bank. *Virtual currency schemes — a further analysis.* ECB Report; February 2015:1–37.

[7] URL: https://www.fca.org.uk/firms/payment-services-regulations-e-money-regulations (accessed on 23.09.2019).

[8] URL: https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html (accessed on 23.09.2019).

[9] European Central Bank. *Virtual currency schemes — a further analysis.* ECB Report; February 2015:1–37.

to describe both the aspect of value and that of the inherent or in-built mechanisms ensuring that value can be transferred.

The International Monetary Fund (IMF) also does not provide a strict definition of cryptocurrency. However, according to the IMF, cryptocurrencies are generally not currencies but rather assets and high-risk investments[10].

In accordance with Article 2 of the Draft Federal Law of 25.01.2018 "On digital financial assets" of the Ministry of Finance of the Russian Federation, "cryptocurrency is a type of digital financial asset created and recorded in a distributed ledger of digital transactions by participants of this ledger in accordance with the rules for maintaining a digital transaction ledger" [11].

The question comes up: which of the above properties of money do cryptocurrencies perform?

Today, cryptocurrencies partially fulfill the function of a means of payment, since certain groups of economic agents are ready to accept them as payment for goods and services. According to the BIS report[12], "money is an indispensable social convention backed by an accountable institution within the State that enjoys public trust". However, to use a certain instrument as a means of payment, it is more important that there is an analogue of the "social convention" between agents than the validity of such a means of payment[13].

Today, cryptocurrencies are not secure savings or a unit of account due to the high volatility of the main cryptocurrencies. The exchange rate of cryptocurrency is based on supply and demand. In this regard, two aspects influence the high volatility of exchange rates: first, the high speculative component in demand and, second, the limited cryptocurrency supply, i.e. the complexity of elastic expansion of its supply in response to market demand. For this reason, cryptocurrencies today cannot be a reliable means of preserving purchasing power. The cryptocurrency volatility is also explained by the fact that cryptocurrencies are an inconvenient unit of account due to frequent price revisions expressed in units of cryptocurrencies. Besides, the high volatility of the exchange rate (coupled with the fact that cryptocurrencies are no one's obligation[14]) discredits cryptocurrencies, which also does not contribute to their distribution as "good money"[15].

Unlike "money", cryptocurrencies perform a unique function of transferring and storing information. First, cryptocurrency blockchains store all secure and immutable transaction information. In this regard, this data source can always be addressed to resolve any issues. Second, many cryptocurrencies are specifically designed so that writing smart-contracts easy. This allows not only to get rid of intermediaries and reduce time and money costs for many types of transactions, but also record information about these transactions in blockchain, which cannot be changed by unscrupulous counterparties.

The BIS defined cryptocurrency as an asset, calling a more detailed consideration of the characteristics that formally satisfy assets in general and financial assets in particular. According to the Organization for Economic Co-

[10] International Monetary Fund. *Money, transformed. The future of currency in a digital world.* Finance and development. 2018;55(2).

[11] Ministry of Finance of Russia. Draft Federal Law of 05.22.2018 "On Digital and Financial Assets". January 2018. URL: https://www.minfin.ru/ru/document/%3Fid_4%3D 121810 (accessed on 23.09.2019).

[12] Bank of international settlements, CPMI. *Central bank digital currencies.* 2018.

[13] In certain periods, e.g., hyperinflation, the money issued by the central bank may lose the trust of economic agents due to a significant and continuing decline in purchasing power. In such cases, agents may switch to more reliable instruments that in terms of preserving the purchasing power (not fixed by law as a means of payment) for transactions or barter.

[14] There are two ways to issue cryptocurrencies: decentralized — by a network of users, and centralized — by one or a group of agents. Regardless of the method of issue, "traditional" cryptocurrencies are not an obligation of any economic agent, unlike the money of the central bank.

[15] Individual national currencies show high fluctuations in prices (exchange rates) of one currency regarding another in relatively short intervals. In fact, any good or durable asset that can be saved for future use is a potential store of value, and in this regard, some of them are more reliable than money.

Table 1

Comparative analysis of cryptocurrencies as money and asset

Features	Money	Assets	Financial assets	Cryptocurrencies
Store of value	Yes	Yes	Yes	No
Means of payment	Yes	No	No	Partially
Unit of account	Yes	No	No	No
Granting ownership	No	Yes	Yes	Yes
Providing the owner with economic benefits through storage or use	Possible*	Yes	Yes	Possible
Is the obligation of the other party	Yes	No	Yes	No
Information transfer and storage function	No **	No	No	Yes

Source: compiled by the authors.

* Assuming that this is the narrowest monetary aggregate (M0), the benefit may occur during deflation. The benefit of storing components of wider monetary aggregates is due to the presence of interest income.

** Except for considering the concept "money is memory", according to which possessing money by an economic agent is the evidence that s/he had conscientiously fulfilled his obligations to the counterparty.

operation and Development (OECD)[16], assets are entities functioning as stores of value and from which economic benefits may be derived by their owners by holding them, or using them, over a period of time. As mentioned earlier, cryptocurrency is not a secure saving, in other words, it does not have stable purchasing power over a long period of time. At the same time, the issue of property rights in the context of cryptocurrency is controversial and depends on the legislative regulation in each country.

Cryptocurrencies often do not provide the owner with a stream of payments, unlike land, real estate, or stocks and bonds[17]. The argument that is usually used to explain the lack of intrinsic (fundamental) value in cryptocurrencies, which is confirmed in some econometric studies, in particular by work [4].

At the same time, the demand for cryptocurrency is largely related to the expectations of agents regarding the increase in its exchange rate, and in this context, cryptocurrencies can provide their owners with the economic benefits of storage. Financial assets, as defined by the OECD[18], in addition to the above characteristics, are someone else's obligation; this condition is not satisfied for cryptocurrencies in their classical sense. Thus, cryptocurrencies satisfy individual properties of assets in their broad interpretation. Today, verifying how "standard" pricing models for financial assets can describe cryptocurrencies is a popular area of research in applied finance [5–9]. In particular, the works test the capabilities of the CAPM, APT or multifactor models to adequately describe the dynamics of cryptocurrency prices. The literature also raises the question of risk diversification of an investment portfolio with cryptocurrencies [10, 11].

Table 1 illustrates a comparison of cryptocurrencies with money and assets.

Howmuch.net data[19] also proves the negligible share of cryptocurrencies compared to other types of assets. Nevertheless, cryptocurrencies

[16] OECD. Glossary of Statistical Terms (Assets). URL: https://stats.oecd.org/glossary/detail.asp? ID=2974 (accessed on 23.09.2019).

[17] Note, that the stellar cryptocurrency implies an increase in coins on the account at a rate of 1% per year.

[18] OECD. Glossary of Statistical Terms (Financial Assets). URL: https://stats.oecd.org/glossary/detail.asp? ID=961 (accessed on 23.09.2019).

[19] URL: https://howmuch.net/articles/worlds-money-in-perspective-2018 (accessed on 23.09.2019).

have become a very important topic discussed in recent years in the literature, and their development prospects are an open question.

CRYPTOCURRENCIES VS TRADITIONAL PAYMENT SYSTEMS

Our analysis shows that cryptocurrencies can be used as a means of payment, but they cannot serve as a reliable unit of account or a means of saving.

In addition to the fundamental problem of trust in cryptocurrencies, which are no one's obligations, and inelasticity or insufficient flexibility of the offer by some cryptocurrencies, other limitations of cryptocurrency payment systems are also highlighted [12–14].

The first problem is associated with the low transaction speed in blockchain of most cryptocurrencies. For example, according to the BIS[20] and howmuch.net, Bitcoin is able to conduct only 7 transactions per second, while the traditional Visa and Paypal payment systems — 24,000 and 193, respectively. On the other hand, such projects as Ripple, EOS and Futurepia are capable of carrying out 1,700.3 thousand and even 300 thousand transactions per second, respectively, which indicates their high potential in this area.

The next limitation of cryptocurrency systems is associated with insignificant volumes of transactions compared to payments made through retail and wholesale payment systems around the world. In addition, there is a fee volatility due to hardware restrictions on the amount of information per one block: increasing demand for transfers in the system leads to increasing fees.

The composition of market participants who are ready to use cryptocurrency systems is limited[21], and the energy footprint required for cryptocurrency mining is high. The increase in computing power is accompanied by an equivalent increase in electricity consumption. According to the results by O'Dwyer and Malone [15], the entire mining network is on par with Ireland for electricity consumption in 2009–2014. In fact, the authors concluded that the monetary cost of the energy and equipment should be compared to the reward for miners. According to digiconomist.net estimates, in 2017, 32.7 TWh were spent on Bitcoin mining, which is comparable to the annual energy consumption of Serbia, Denmark or Belarus, and 11.1 TWh — on Ethereum mining, which is approximately equal to the energy consumption of Zambia or Lithuania. As a comparison, in 2017, Moscow spent 105 TWh. Currently, the annual electricity consumption for Bitcoin mining is 73.12 TWh, which is comparable to Austria's energy consumption[22].

It is also important that traditional payment systems consume much less electricity than the Bitcoin payment system or any other blockchain payment system based on PoW, which implies mining. For example, the cost of energy consumption per transaction for Bitcoin is equal to that of almost 600 thousand Visa transactions[23].

Information should be stored if payments will be made using blockchain. According to the BIS estimates[24], starting from 1 July 2018, all electronic non-cash retail transactions[25] are processed via a cryptocurrency, hypothetical ledger size for nationwide retail cryptocurrency in the Euro area, China and the United States will be more than 45, 80 and 105 TB by 2021, respectively. A problem will arise if this information needs to be stored in all blockchain nodes.

[20] Bank of international settlements. BIS *Annual Economic Report*. 2018.

[21] At the same time, the largest banks, in particular Barclays and HSBC, declare their interest in the new technology and participate in the project to create an international payment system based on blockchain.

[22] URL: https://digiconomist.net/bitcoin-energy-consumption (accessed on 23.09.2019).

[23] URL: https://www.statista.com/statistics/881541/bitcoin-energy-consumption-transaction-comparison-visa/ (accessed on 23.09.2019).

[24] Bank of international settlements. BIS *Annual Economic Report*. 2018.

[25] The calculations were made not for all countries of the Euro area, but only for France, Belgium, the Netherlands, Germany and Italy.

Another serious issue is whether use and storage of cryptocurrencies is reliable and safe regarding no-failure operation of the technology? People should be sure of the low vulnerability of cryptocurrencies to fraud and malfunctions. So far, the technical security of distributed ledger technology has not been tested on a large scale. At the same time, changing the ledger with a large number of nodes will be more difficult, since a huge number of copies will have to be manipulated at the same time. On the other hand, the consensus protocol can be manipulated by a malicious participant (group of participants) who controls the majority of votes or computing power ("consensus capture"). Moreover, cryptographic methods that are secure today may be hacked in the future if computing power continues to increase. Bruno Huttner [16] also noted anticipated threats to blockchain technology and digital currencies from quantum computers. The advent of quantum computing over the next 10–15 years current cryptography might not be so secure anymore. In other words, as a result, quantum computers may well bypass the existing security system that underlies blockchain and digital currencies.

The anonymity of cryptocurrencies (or pseudonymity) carries the risk of potential money laundering or terrorist financing. If the law does not require this, user information can be protected from disclosure to third parties and governments, while criminals can be held back by the risk of investigation and prosecution. Banks whose business will be associated with cryptocurrencies will have to comply with the Know Your Customer rule and the requirements for combating money laundering and terrorist financing when conducting their operations with cryptocurrencies.

Nevertheless, it is possible to list benefits of blockchain based payment systems vs traditional payment systems, mentioned in the literature[26]. The first benefit is the lack of need for a central authority. In traditional payment systems, there is an authority like a bank that is able to control all customer's actions through their system. Banks have all the information about customer payments and other personal information. There is a potential risk that banks may share this information with third parties. Blockchain-based payment system is more secure and transparent for customers in terms of data protection. However, state bodies are able to identify people in case of suspicions or evidence of their involvement in illegal activities.

The second benefit is the lack of need for a high budget for security. Traditional systems, including banks and payment system operators (like Visa or Mastercard) spend vast sums of money in order to protect the customer data (they build servers, security teams and control teams that have a high effect in their budget management). Blockchain system carries the risks of a "51% attack" or a "deep attack", but such a hack for criminals is also associated with high costs. Therefore, if the cryptocurrency system is large enough and there are many users in the blockchain payment system, it can be considered safe at the current time.

The third benefit of blockchain payment systems is instant cash-out. This argument is controversial. Banks require a settlement time to cash-out company's revenue, while blockchain payment systems provide an easier and faster cash-out process without any settlement rate. Of course, this does not apply to the customer's cash-out from their payment card linked to the bank account. A wide network of ATMs around the world makes it possible to receive cash 24/7 at minimal cost.

The fourth benefit is the fact that fees in cryptocurrency systems are acceptable and reasonable. However, this argument is also controversial. On the one hand, traditional payment systems include various payment intermediaries: a payment system operator, a customer's bank and a seller's bank, and all of them require a commission and transaction fees. In a decentralized system, i.e. in blockchain payment sys-

[26] URL: https://medium.com/menapay/traditional-payment-systems-vs-blockchain-payment-systems-1fbccff56b87 (accessed on 23.09.2019).

tems, transaction fees are determined by the participants — supply and demand in the market. It is expected that this method should lead to a reduction in commission fees compared to traditional payment systems. On the other hand, one of the main problems of cryptocurrency markets is the high volatility of commissions. Moreover, during periods of abnormally high prices for cryptocurrencies, commission fees also increase sharply. For example, transaction fees in the Bitcoin system reached $ 55 as of December 22, 2017 — the peak cryptocurrency price period[27].

The fifth benefit is the ability to make fast international transfers. Especially in cross-border transactions, traditional payment systems fail in giving a fast service. Blockchain helps its customers to make a lot faster transactions between peers in international payments.

There are also several developed international payment models based on central bank digital currencies (CBCD)[28]. In wholesale payment systems of central bank digital currencies, like in traditional wholesale payment systems using reserves for settlement transactions, there are credit, settlement, operational and liquidity risks. The relationship of these risks in payment systems based on central bank digital currencies is currently unknown and may significantly differ from the distribution of risks in traditional payment systems. Mitigation or optimization (compromise) of risks will largely depend on the technical solutions chosen to make payments (issuing "protocols", an intraday liquidity policy, interest payments on central bank digital currencies, etc.). It is assumed that technical solutions can reduce credit, settlement, operational and liquidity risks in the wholesale payment systems of central bank digital currencies. According to Project Ubin[29], distributed ledger technology is a potential opportunity to improve domestic securities transactions by offering the calculations of Delivery-vs-Payment (DvP) in cases of significant improvements in cross-border payments (payment versus payment) and securities transactions (DvP).

Thus, the infrastructure of traditional and cryptocurrency-based payment systems reveals the main differences between them, as well as advantages and disadvantages.

In the literature, as well as among economists and market participants, the comparative advantages and disadvantages of various cryptocurrency payment systems are discussed. Cryptocurrencies Bitcoin, Ripple, and Ethereum are the most interesting to compare. Ripple is the one that most corresponds to the payment system in the traditional sense. The latter dominates both Bitcoin and Ethereum in terms of transaction speed (analogue of RTGS, real-time gross settlement system, payment system with currency exchange) and coin scalability. Ethereum is a decentralized platform that launches smart contracts, so its scope is not limited to payments. As for Bitcoin, it is still the main cryptocurrency for payments and investment.

The following sections are devoted to the view of economic theory on the concept of cryptocurrency.

TRADITIONAL MONETARY-FINANCIAL MODELS AND CRYPTOCURRENCIES

Attempts to define cryptocurrencies in terms of usual established economic and financial categories led to a discussion to what extent cryptocurrencies are private money. First of all, it is about comparing them with historical examples of means of payment, as well as with Hayek private bank money [17] in the context of

[27] URL: https://bitinfocharts.com/comparison/bitcoin-transactionfees.html (accessed on 23.09.2019).

[28] See Bank of Canada, Bank of England. *Cross-border Interbank payments and Settlement. Emerging opportunities for digital transformation.* November 2018. A detailed discussion of central banks digital currencies is beyond the scope of this paper.

[29] Bank of America, Merrill Lynch, BCS Information Systems, Credit Suisse, DBS Bank, HSBC, J.P. Morgan, Mitsubishi UFJ Financial Group, OCBC Bank, R 3, Singapore Exchange, and UOB Bank. *The future is here. Project Ubin: SGD on Distributed Ledger*. 2017.

Table 2

Comparative analysis of Hayek money and cryptocurrencies

	Hayek money	Cryptocurrencies
Currency issuance	Centralized	Decentralized
Is it anyone's obligation?	Commercial issuing bank's	No
Currency deissuance	Possible	Depends on protocol
Interest rate	Yes	Not at the moment, since the relevant credit and deposit operations were not distributed

Source: compiled by the authors.

the potential crowding out of state money with "private" ones[30].

Hayek wrote this work when reducing inflation was an acute problem and, according to Hayek, could not be solved due to the seigniorage the authorities resorted to. The author believed that the regulation of monetary issuance leads to loss of efficiency of the monetary system, and that currency should be considered an ordinary commercial product and produced in a competitive (market) way. In the result of the competition, there will remain only the currencies that will best fulfill the functions of money, i.e. serve as a means of payment and store their value in time. *Table 2* compares Hayek money and cryptocurrencies. It is clear that they formally represent different economic phenomena, mainly due to the fact that most cryptocurrencies are no one's obligation, unlike the money of private commercial banks.

According to formal definitions of cryptocurrencies, as well as to what we see in practice, cryptocurrency is no one's obligation. Nevertheless, some private digital currencies have appeared on the market (also called cryptocurrencies by their issuers), and their exchange rate is fixed in some national currencies. In other words, there are exceptions when a digital currency issuer declares its obligation to exchange digital coins for another asset, e.g. the US dollar. Cryptocurrencies that have some kind of guarantee regarding the price volatility are called stablecoins. Centralized stablecoins are cryptocurrencies with a central issuer that is involved in the production of crypto tools and the storage of their security in their accounts. These currencies can be divided into two groups:

1. Guaranteed by fiat currency.
2. Guaranteed by any traded goods or asset (meaning exchange goods).

There are also so-called decentralized stablecoins. These are cryptocurrencies guaranteed by another cryptocurrency (non-fiat currency or an asset, as discussed above).

NEW MONETARISM, ECONOMICS OF PAYMENTS AND CRYPTOCURRENCY

We reviewed the discussion regarding the economic nature of cryptocurrencies and crypto assets. The question comes up whether there are any formal models explaining potential benefits and consequences of using cryptocurrency? Today, there are only a few theoretical works and formal models describing the behavior of cryptocurrency and the cryptocurrency market. The reason for this is that traditional

[30] Speaking of historical examples of private money, we mean, for example, debt receipts in China of the X–XII centuries, money secured by silver in Japan of the XV–XVI centuries, banknotes in the form of receipts confirming the deposit of metal money in Europe (Venice, Holland) XVII century. Crowding out central bank money by private money is based on the idea that inflation, due to coin corruption or seigniorage, reduces the purchasing power of state money and discredits it. One of the most striking examples of mass corruption of coins and high inflation is the XVII century coin crisis in central European countries located on the territory of modern Germany, called "Kipper- und Wipperzeit" (literally "Tipper and See-saw time"). For more information on the origin of paper money and central banks, see work [18].

economic theory does not have the tools necessary to work with cryptocurrencies. The only theoretical exception that analyzes cryptocurrencies within strict models is the new monetarist approach, and specifically one of its sectors, the economics of payments[31].

In his work [23], Waknis built a dual currency version of Lagos & Wright money search model [24]. His goal was to answer the fundamental question of monetary theory: whether currency can be efficiently provided by private competitive money suppliers[32] and whether competitive money supply is more efficient than a monopoly? This is an important issue both theoretically and practically due to the recent emergence of various financial instruments and cryptocurrencies, which can serve as a means of payment and to some extent savings, i.e. potentially act as money. The competition between these instruments raises the question of an effective way to conduct transactions and the best monetary policy in the world with a competitive money supply. Waknis presented a model with a centralized market as an infinitely repeating game between a long-lived player (suppliers of money) and a short-lived player (continuum of agents).

There are two sub-periods:

1. A day sub-period where special goods are traded in a decentralized market. The decentralized market is characterized by trading frictions and hence money gets valued for the liquidity services it provides.

2. A night sub-period where a general good is traded in a centralized Walrasian market. The night trading is anonymous and is used by agents to trade in the general good and rebalance their portfolios.

The economy is characterized by imperfect memory and record keeping to rule out credit transactions[33]. To describe the equilibrium we begin by describing the value functions, taking as given the terms of trade and distribution of monies. The state variables for the individual include his real money balances and a vector of aggregate states and the growth rates of currency R and B respectively; ϕ^R and ϕ^B are the value of money in currency R and B respectively, in the centralized market[34]. The value functions of agents depend on their entry into two existing markets: centralized and decentralized. Value functions also depend on standard "search and coincidence" parameters: a probability of a meeting, a single coincidence meeting, and and that of a barter exchange.

There are two monetary authorities, BankR and BankB issuing R and B currency respectively. New money is issued by the money suppliers in the centralized market to consume the general good[35]. The author models the choice of monetary growth rate under no commitment as an infinitely repeated game. Because the short lived player optimizes myopically i.e., is concerned only with optimizing current period consumption and the money that it carries out of the centralized market — it always plays Nash response and hence the equilibrium outcomes lie on its best response function. As the money suppliers' are long run players, utility maximization amounts to choosing the money growth rate to maximize the average discounted payoff.

In the centralized market, the game is modelled as dynamic with two money suppliers, maximizing their utility, and a continuum of economic agents. The author showed that the Nash equilibrium in a static game gives the highest inflation tax, similar to the case with one issuer of money in the work by Waknis [27]. In the general case of infinitely repeated games, there are multiple equilibria. The competition between money suppliers and the fact that agents play only Nash responses transforms the centralized market game to a dilemma between the two money suppliers.

[31] For more details, see works by Williamson S. and Wright R. [19, 20], and by Nosal E. and Rocheteau G. [21, 22].

[32] In this case, private competitive money supplier include cryptocurrency suppliers.

[33] For more details, see Kocherlakota [3] and Wallace [25].

[34] It represents the units of general good that be bought by one unit of the respective currency in the centralized market.

[35] A privilege derived from access to record keeping technology [26].

If both the money suppliers are patient enough, then the equilibrium with lowest inflation tax (cooperative equilibrium) is weakly renegotiation proof, implying that currency competition is likely to generate a low inflationary outcome. This means that there are conditions under which competition between monies is preferable because it can lead to low inflation, which is in line with Hayek's ideas discussed earlier.

CONCLUSIONS

The aim of this work was to write both a comprehensive and an exhaustive review disclosing the essence of cryptocurrencies, their functions, as well as the problems and benefits associated with their use. Special attention was paid to the technological basis of cryptocurrency issuance, since the features of issuance protocols are the starting point for discussing substantive issues related to the functioning of cryptocurrencies.

Despite the lack of a single definition and understanding of the essence of cryptocurrencies in the literature, the analysis allows us to make the following conclusions. First, cryptocurrencies do not satisfy all the characteristics of money and assets. Second, cryptocurrencies today are speculative assets that partially fulfill the function of a means of payment. Third, cryptocurrencies can have significant development prospects in terms of making payments, storing and transmitting information, primarily due to the innovative technology on which they operate.

Despite their limitations (some cryptocurrencies currently do not have technical solutions) and "internal" reliability of the cryptocurrency payment system, cryptocurrencies are of significant interest not only to investors, the public, but also to monetary policy authorities. The reason is that making payments by distributed ledger technology can reduce transaction costs and has an inbuilt function of transmitting and storing information. The growth in demand for crypto payments led to a situation where not only commercial, but also central banks consider issuing their own digital money.

The main condition for trust in any currency, including cryptocurrency, and its widespread use by agents is the stability of its purchasing power (for more details see [28]). Although the analysis based on formal models shows that under certain conditions suppliers of private money adhere to issuing methods leading to low inflation, the very nature of cryptocurrencies contradicts the idea of centralized responsibility for the financial system. Thus, cryptocurrencies cannot be regarded as a replacement for the existing monetary system, at least for now.

ACKNOWLEDGMENT

The authors are grateful to the referee for valuable comments and suggestions.

REFERENCES

1. Preneel B. The first 30 years of cryptographic hash functions and the NIST SHA-3 competition. In: Pieprzyk J., ed. Topics in cryptology — CT-RSA 2010. The 10th Cryptographers' track at the RSA conference (San Francisco, CA, 1–5 March, 2010). Berlin, Heidelberg: Springer-Verlag; 2010:1–14.
2. Mazières D. The stellar consensus protocol: A federated model for internet-level consensus. Stellar Development Foundation. 2015. URL: https://www.stellar.org/papers/stellar-consensus-protocol.pdf
3. Kocherlakota N. Money is memory. *Journal of Economic Theory*. 1998;81(2):232–251. DOI: 10.1006/jeth.1997.2357
4. Cheah E.-T., Fry J. Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin. *Economics Letters.* 2015;130:32–36. DOI: 10.1016/j.econlet.2015.02.029
5. Ciaian P., Rajcaniova M., Kancs A. The digital agenda of virtual currencies. Can BitCoin become a global currency? *Information Systems e-Business Management*. 2016;14(4):883–919. DOI: 10.1007/s10257–016–0304–0

6. Hayes A. The decision to produce Altcoins: Miners' arbitrage in cryptocurrency markets. *SSRN Electronic Journal*. 2015. DOI: 10.2139/ssrn.2579448
7. Hayes A. Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing Bitcoin. *Telematics and Informatics*. 2017;34(7):1308–1321. DOI: 10.1016/j.tele.2016.05.005
8. Sovbetov Y. Factors influencing cryptocurrency prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero. *Journal of Economics and Financial Analysis*. 2018;2(2):1–27. DOI: 10.1991/jefa.v2i2.a16
9. Liu Y., Tsyvinski A. Risks and returns of cryptocurrency. *SSRN Electronic Journal*. 2018. DOI: 10.2139/ssrn.3226952
10. Dyhrberg A. H. Bitcoin, gold and the dollar — A GARCH volatility analysis. *Finance Research Letters*. 2016;16:85–92. DOI: 10.1016/j.frl.2015.10.008
11. Carpenter A. Portfolio diversification with Bitcoin. *Journal of Undergraduate Research in Finance*. 2016;6(1):1–27. URL: https://jurf.org/wp-content/uploads/2017/01/carpenter-andrew-2016.pdf
12. Huberman G., Leshno J., Moallemi C. Monopoly without a monopolist: An economic analysis of the bitcoin payment system. Bank of Finland Research Discussion Paper. 2017;(27). URL: http://ipl.econ.duke.edu/seminars/system/files/seminars/1874.pdf
13. Easley D., O'Hara M., Basu S. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*. 2019;134(1):91–109. DOI: 10.1016/j.jfineco.2019.03.004
14. Abadi J., Brunnermeier M. Blockchain economics. Centre for Economic Policy Research. CEPR Discussion Papers. 2018;(13420). URL: https://scholar.princeton.edu/sites/default/files/markus/files/blockchain_paper_v3g.pdf
15. O'Dwyer K., Malone D. Bitcoin mining and its energy footprint. In: 25th IET Irish signals & systems conf. 2014 and 2014 China-Ireland int. conf. on information and communications technologies (ISSC 2014/CIICT 2014). (Limerick, Ireland, 26–27 June 2014). Limerick: University of Limerick; 2014:262–268. URL: http://karlodwyer.com/publications/pdf/bitcoin_KJOD_2014.pdf
16. Huttner B. Quantum threats and possible solutions for blockchains and digital currencies. In: World Summit on the Information Society Forum (WSIS Forum). Session 304: Central Bank issued digital currency: Challenges for security and interoperability. (Geneva, 19–23 March, 2018). 2018:19–23.
17. Hayek F. Denationalization of money — The argument refined: An analysis of the theory and practice of concurrent currencies. London: The Institute of Economic Affairs; 1976. 146 p.
18. Moiseev S. History of central banks and paper money. Moscow: Veche; 2015. 536 p. (In Russ.).
19. Williamson S., Wright R. New monetarist economics: Models. In: Friedman B. M., Woodford M., eds. Handbook of monetary economics. Amsterdam: North Holland; 2010;3A:25–96.
20. Williamson S., Wright R. New monetarist economics: Methods. Federal Reserve Bank of Minneapolis. Research Department Staff Report. 2010;(442). URL: https://www.minneapolisfed.org/research/sr/sr442.pdf
21. Nosal E., Rocheteau G. The economics of payments. Federal Reserve Band of Cleveland. Policy Discussion Paper. 2006;(14). URL: https://www.clevelandfed.org/en/newsroom-and-events/publications/discontinued-publications/policy-discussion-papers/pdp-0614-the-economics-of-payments.aspx
22. Nosal E., Rocheteau G. Money, payments, and liquidity. Cambridge, MA: The MIT Press; 2011. 504 p.
23. Waknis P. Competitive supply of money in a new monetarist model. Munich Personal RePEc Archive. MPRA Paper. 2017;(75401). URL: https://mpra.ub.uni-muenchen.de/75401/1/MPRA_paper_75401.pdf
24. Lagos R., Wright R. A unified framework for monetary theory and policy analysis. *Journal of Political Economy*. 2005;113(3):463–484. DOI: 10.1086/429804
25. Wallace N. Whither monetary economics? *International Economic Review*. 2001;42(4):847–869. DOI: 10.1111/1468–2354.00137
26. Fernández-Villaverde J., Sanches D. Can currency competition work? NBER Working Paper. 2016;(22157). URL: https://www.nber.org/papers/w22157.pdf

27. Waknis P. A Leviathan central bank: Modeling Seigniorage in a money search model. *Economics Letters*. 2014;125(3):386–391. DOI: 10.1016/j.econlet.2014.10.027
28. Schnabel I., Shin H. Money and trust: Lessons from the 1620s for money in the digital age. BIS Working Papers. 2018;(698). URL: https://www.bis.org/publ/work698.pdf

ABOUT THE AUTHORS

Elena V. Sinel'nikova-Muryleva — Can. Sci. (Econ.), Senior Researcher, Institute of Applied Economic Research, Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russia
el.sinelnikova@gmail.com

Kirill D. Shilov — Researcher, Institute of Applied Economic Research, Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russia
shilovkd@gmail.com

Andrei V. Zubarev — Can. Sci. (Econ.), Senior Researcher, Institute of Applied Economic Research, Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russia
texxik@gmail.com

Authors' declared contribution:
Sinel'nikova-Muryleva E.V.— articulation of the issue, development of the concept of the article, critical analysis of the literature, logical structuring of the material, drawing conclusions.
Shilov K.D.— collection of statistical data, tabular and graphical presentation of the results, drawing research conclusions.
Zubarev A.V.— research concept development, drawing research conclusions.

The article was submitted on 08.10.2019; revised on 22.10.2019 and accepted for publication on 28.10.2019. The authors read and approved the final version of the manuscript.