ORIGINAL PAPER

DOI: 10.26794/2587-5671-2019-23-6-26-35
UDC 330.88:004.738.5:336.747.5(045)
JEL O33

Current State and Development Trends of Blockchain Technology in the Financial Sector

G.O. Krylov[a], **V.M. Seleznev**[b]
[a] Financial University, Moscow, Russia; [a] National Research Nuclear University MEPhI, Moscow, Russia; [b] JSC LatCard, Riga, Latvia
[a] https://orcid.org/0000-0001-8145-1994; [b] https://orcid.org/0000-0003-4521-0290

ABSTRACT

The article analyzes the main reasons for the slow adoption of blockchain technology, in particular, in the financial sector. The authors critically analyzed the main declared properties of blockchain technologies: trust, security, decentralization, immutable data storage, lack of intermediaries, hardware protection against attacks, and openness. The aim of the study are to show that these blockchain properties are overestimated, the expectations of its adoption are inflated, and the delays in its adaptation outside of cryptocurrencies, in particular, in the financial sector, are natural. The article is based on a methodology for the qualitative and quantitative analysis of scientific publications and statistical sources on the blockchain adaptation from the perspective of the theory of diffusion of innovations, the conditions and the specifics of economic and sociological approaches for consensus-building. The study resulted in the following new systemic findings. Blockchain and distributed ledgers are not fundamentally new technologies. In general, they do not have the properties of the immutable data storage, trust, anonymity, low transaction and adoption costs. All current consensus technologies have fundamental faults. Cryptocurrency technology is original, but it was a private experimental solution to a specific ideological problem of the libertarian political agenda. Consensus does not provide trust. Delayed blockchain adoption, in particular in traditional financial institutions, is natural, since the technology does not show better results than current digital solutions, and traditional economic institutions have greater public trust. The practical implications of the findings are that they may be used by investors.

For citation: **Krylov G.O., Seleznev V.M. Current state and development trends of blockchain technology in the financial sector. *Finance: Theory and Practice*. 2019;23(6):26-35. DOI: 10.26794/2587-5671-2019-23-6-26-35**

INTRODUCTION

The blockchain market entered 2019, the eleventh year since the publication of the Bitcoin manifest, with multidirectional trends. Speculative capital lost interest in blockchain. Since the end of 2018, investment in blockchain startups has fallen by 60%[1]. From January to June 2019, investment in ICOs went down by 17.8 times compared to the same period in 2018 (*the figure* shows the investment schedule in ICOs). At the same time, the corporate sector and strategic investors were keen on supporting blockchain technologies, or, as they say in the corporate segment, distributed registry technologies.

Announcements of technology testing or strategic vision of blockchain technology positively affect the capitalization of large companies [1]. Today, it seems impossible to be a technology leader and not invest in blockchain projects[2]. The above factors might have pointed to blockchain's increased maturity, if there were any signs of mass adaptation of blockchain outside of Bitcoin and cryptocurrencies. In this article, we analyze the reasons for the slow adaptation of blockchain technology (in particular, in the financial sector) and

[1] According to the study by CBInsights (CB Information Services). URL: https://www.cbinsights.com/research/report/blockchain-trends-opportunities/ (accessed on 10.10.2019).

[2] According to the survey of 1386 company executives with a profit of more than $ 0.5 billion conducted by Deloitte in the winter-spring of 2019, 77% of respondents believe that the company will lose its competitive advantage if it does not adopt blockchain technology.URL: https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html (accessed on 10.10.2019).

the justification of expectations from its widespread adoption.

BLOCKCHAIN'S DECLARED PROPERTIES

In his opus magnum "Blockchain Revolution" [2], one of the most important apologists for blockchain, the godfather of the "digital economy", Don Tapscott formulated most general expectations from blockchain introduction, placing them in the context of global digitalization. According to Tapscott and other technology evangelists [3, 4], blockchain will allow:

- to create a new sharing economy, where all economic activities take place with no intermediaries;
- to create a new, fully inclusive, high-speed financial system with zero overhead costs;
- to protect economic rights around the world;
- to root out corruption and bureaucracy;
- to protect copyrights (in the broad sense, the rights of the creator) and creators to receive remuneration directly;
- to educate a new type of entrepreneur — a blockchain entrepreneur — and to create a new honest capitalism by transforming corporations;
- to make the entire human environment high-tech by "reviving" and connecting all the objects together;
- to realize true democracy from the people and for the people.

According to the apologists, blockchain is the solution to most of the major problems of human civilization. In particular, the following benefits for financial organizations are expected after blockchain implementation:

- a significant reduction in IT infrastructure costs by replacing the back office with blockchain [5];
- cost reduction of interbank payments;
- improving the security of banking data;
- faster transaction processing;
- smart contracts will help to avoid mistakes and provide financial services with a new quality;
- banking will become more open and transparent [6].

These forecasts are based on immanent properties of the technology such as:

- trustlessness;
- peer-to-peer network;
- built-in cryptographic security mechanisms;
- economic inexpediency of attacks on the system;
- anonymity;
- immutable data storage;
- openness and free of charge.

There is no surprise that these promises, supported by information about the success of the first cryptocurrency Bitcoin, have amassed $ 7.5 billion in investment funding since 2012, with $ 4 billion of them invested in 2018[3], which is at least 4 times the total investment in quantum computing for a comparable period[4]. So, why does the implementation of blockchain slow down despite such abundant funding?

BLOCKCHAIN AS A "FOUNDATIONAL TECHNOLOGY"

One of the most common explanations for this phenomenon is that blockchain is declared as foundational technology [7], because "it has the potential to create a new foundation and principles for our economic and social systems". In this sense, blockchain is compared to the main Internet protocol TCP/IP, and its main application is cryptocurrency with e-mail, the main application of TCP/IP in 1975.

Forecasts for blockchain development are similar to those of the Internet. First, there will come local private solutions, similar to corporate email; then, blockchain applications will replace the traditional ones, similar to Internet applications; finally, quantity will turn into quality, and a new, smart contract-based reality will be created. According to this concept, we should wait for the breakthrough and experi-

[3] Data by Statista.com. URL: https://www.statista.com/statistics/621207/worldwide-blockchain-startup-financing-history/ (accessed on 10.10.2019).

[4] Data by CB Insights CB Insights. URL: https://www.cbinsights.com/research/report/quantum-computing/ (accessed on 10.10.2019).

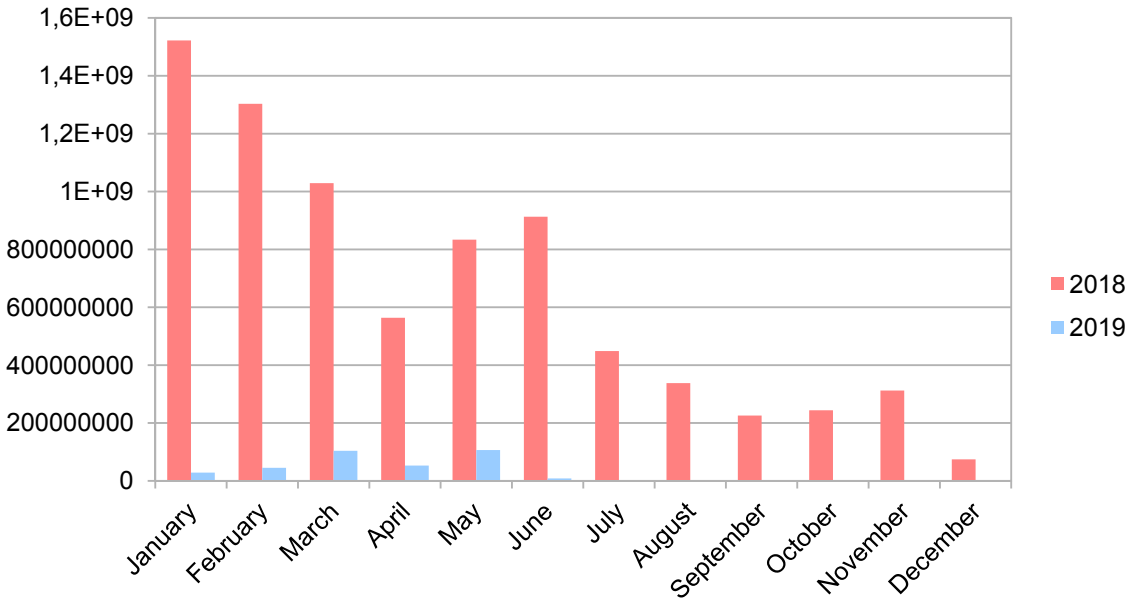

Fig. **ICO investments in 2018–2019 (the 1st half)**

Source: data visualization by the author based on icodata.io data.

* URL: https://www.icodata.io/stats/2018; https://www.icodata.io/stats/2019 (accessed on 10.10.2019).

ment with applying blockchain in different industries.

However, calling blockchain a potentially foundational technology and "the new Internet" seems to be too simplified. First, it is easy to see (for example, in the relevant Wikipedia articles) that from the very beginning the Internet had numerous practical applications besides e-mail. FTP file transfer protocols and remote access to Telnet systems emerged simultaneously with e-mail and are still widely used. Usenet e-conferences appeared a few years after the e-mail and gained instant worldwide popularity. It was in Usenet where Tim Berners-Lee announced the World Wide Web (www), the present main Internet service. All this happened in less than 10 years after the TCP/IP creation.

The second significant simplification is to call the TCP/IP protocol stack a foundational technology. In historical perspective, the win of this protocol (which, by the way, did not satisfy the theoretical model of network interaction) was largely an accident. Network theorists predicted wins to other protocols. At the same time, it is obvious that the WWW and e-mail could exist on top of the protocols of other networks, for example, X.25. In this case, the packet switching mechanism should be considered the foundational technology.

Although based on the multi-year research and the development of long-established concepts, packet switching was a new technology at the time of creation. The novelty of blockchain is doubtful. Actually, there is not a single new technology in the Bitcoin manifest (the first blockchain document). All the technologies used for blockchain had been long known. Databases based on consensus algorithms (for example, Paxos) have been used since 1989. The binary hash tree was patented by Ralph Merkle in 1979. The Hashcash algorithm was published in 1997 already as a reward system, albeit to protect against e-mail spam. Smart contracts, the fundamental element of modern blockchain technologies, were proposed only in 2015 in connection with the Etherium cryptocurrency. At the same time, smart contracts have existed outside the context of blockchain since 1998. On the average, the technologies underlying blockchain have existed for more than 25 years. Whether they are truly foundational, it is a long enough period to find wide application.

THE THEORY OF DIFFUSION OF INNOVATIONS AND BLOCKCHAIN IMPLEMENTATION

Another argument against the fundamental nature of technology is the analysis based on the theory of diffusion of innovations. It is generally recognized that over the past century, the rates of technology introduction and adoption have been speeding up [8]. It took the Internet 10 years to reach 50% of US households. It took 8 years for cellphones to accomplish 90% penetration. Over the same 10 years, 5% of Americans have hold Bitcoin[5], and in the rest of the world, less than 0.5% of the population uses cryptocurrencies[6]. As noted above, the total global investment in blockchain is quite large. Using the innovation curve by Everett Rogers [9], we note a paradox: investments already correspond to the development level of the "early majority" technology [10, 11] with the level of practical penetration of the "innovators" technology. In other words, investment does not lead to technology penetration. What is this but the evidence of the lack of a sign of the core technology at blockchain?

The final argument against the fact that blockchain is a foundational technology is that it is not based on a scientific breakthrough [12]. A foundational technology always follows a scientific breakthrough: in mathematics or science. Of course, blockchain technology uses a mathematical basis, but it is not based on a breakthrough solution of mathematical problems. Moreover, its development encounters precisely the unresolved mathematical consensus problem.

THE CONSENSUS PROBLEM IN THE SUSTAINABLE SYSTEMS THEORY AND THE SOCIO-ECONOMIC APPROACH TO OVERCOME IT

We will take a closer look at the consensus problems, the base for decentralization — a blockchain's advantage. When analyzing the stability problems of computer systems, Leslie Lamport formulated the main problem, called the "the Byzantine Generals Problem", or the "Byzantine Fault Tolerant" (BFT) [13]. The problem research showed that there are solutions only for particular cases. A consensus, or "Byzantine agreement", is only possible with a finite number of participants, provided that there are fewer intruders in the network than a third of the participants. In any asynchronous system, a consensus is not guaranteed [14].

It was proved that if there are possibilities for quantum computation, the time to reach a consensus using the quantum algorithm will be constant [15]. Therefore, practical algorithms to reach a consensus in computer systems can only be approximate and probabilistic. The paradox is that the solutions of the most popular blockchains to reach a consensus are not strictly mathematical. Consensus-building methods are based on socioeconomic assumptions. The Proof of work (PoW) method used by Bitcoin and Etherium [16] relies on the hypothesis that people interested in the "honest" system functioning will always have more computing power than each attacker individually. At the same time, the interest in honesty among the participants will be determined by the basic human properties of rational selfishness (aka greed), since double-spend attacks will be more expensive than the potential benefits. Finally, it is assumed that 51% of the "non-greedy" miners necessary for the attack will not be able to collude, since the processing power is distributed among thousands of anonymous miners who consider anonymity to be the basic value. Unfortunately, the practice of using Bitcoin proved that these assumptions are not true. Double-spend attacks and a combination of double-spending and Sibyl attacks can be economically feasible [17, 18]. There was a small finite number of miners, and their anonymity was not a value; all the main mining pools are known. Moreover, only 6 companies control 70% of mining, five of them are from the Peo-

[5] According to the data by Bitcoin Market Journal. URL: https://www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/ (accessed on 10.10.2019).

[6] Data by statista.com. URL: https://www.statista.com/statistics/647374/worldwideblockchain-wallet-users/ (accessed on 10.10.2019).

ple's Republic of China[7]. Thus, conspiracy is not only possible, but is quite likely.

Realizing the proof of work challenges, the blockchain community is actively seeking for alternatives to this protocol. For example, Ethereum plans to switch to the Proof-of-Stake consensus algorithm. Unfortunately, this protocol also has drawbacks: it destroys the decentralised network and the fair remuneration system, the richest owners of crypto tokens are privileged to make decisions, and it is impossible to determine the "true" transaction history without an additional source of trust [19]. There are many other practical consensus protocols: Proof of Elapsed Time, Proof of Capacity, Delegated Proof-of-Stake. However, all of them have drawbacks inherent in empirical solutions to complex mathematical problems [20, 21].

BLOCKCHAIN: THE PROBLEM OF DEFINITION

The complexity and unsolved mathematical problems associated with blockchain provides active proponents of the technology with another explanation for the delay in its widespread adoption. In their opinion, the principal challenge is a lack of awareness of the technology and a widespread lack of understanding of how it works. [22]. We agree that some elements of the technology require understanding of the basics of applied mathematics. However, practice shows that it is not too difficult to explain the principles of Bitcoin. Difficulties begin when they try to explain an abstract blockchain. Unfortunately, there is still no good definition of blockchain. Most definitions relate to the fact that a blockchain is a decentralized distributed transaction log with a consensus based on the principle of economic rewards in the form of cryptocurrency. However, today, not all blockchains are decentralized, transaction logs or based on cryptoeconomic principles.

The current tendency to introduce a generalized definition of "distributed ledger" for proprietary, non-public exclusive blockchains (or not blockchains by the new definition) contributes to the confusion. Indeed, it is difficult to explain a technology that has no clear definition.

BLOCKCHAIN AS A DATABASE WITH SPECIAL PROPERTIES

Considering blockchain a distributed database contributes even more to the confusion. Strictly speaking, in the vast majority of cases, blockchain (given the fuzziness of the definition) is not a database at all. First, it does not record the current state of the system (i.e. it is not consistent), and second, it does not ensure data availability [23]. Blockchain is a historical log of all events that changed that status. In the Bitcoin system, for example the current balances are recorded separately. For optimization, in the vast majority of cases, blockchains keep at most the headers of the blocks, not the full blocks. The use of a blockchain does not ensure, per se, that the past history of the system will always be available for checking. For example, the Ripple blockchain is missing approximately 32 thousand blocks at its beginning — because no one felt necessary to save them at the time!

Admitting that blockchain is not a database, but a log, would make it easier to explain it is append-only and does not change data. This property is not so useful. (What will be the cost of the error?). Fortunately (or unfortunately), contrary to claims of many suporters, the blockchain data is not constant per se. Regarding the data in public blockchains, transactions may be cancelled by agreement of the parties or during a limited period, while in exclusive distributed ledgers — by decision of the moderating party.

It is possible to change blockchain both by an external mechanism, a group of attackers who may profit from the attack, and by an internal mechanism, collusion of most legal miners. Moreover, the "legal" kickbacks of Bitcoin occurred at least three times.

In general, blockchain technologies are not so complicated as they are confusing due to simplifications and incorrect analogies. Poor definitions and omissions in explanations endow the tech-

[7] According to the data by BTC.com. URL: https://btc.com/stats/pool?pool_mode=year (accessed on 10.10.2019).

nology with properties that it does not possess, while its fundamental flaws are hidden behind the info noise.

BLOCKCHAIN AS A PRIVATE SOLUTION OF THE IDEOLOGICAL PROBLEM OF LIBERTARIANITY

The next most important argument explaining what holds blockchain back from large scale adoption is the need to train both "blockchain specialists" and masses, which, of course, takes time [24]. In other words, for the mass adoption, literally everyone should understand the basics of discrete mathematics, applied cryptography and learn how to write smart contracts. Finally, the dream of the personal computer development pioneer, Steve Wozniak, must come true, and everybody will become programmers. In the real world, this dream is probably as realistic as the belief that with real democracy any person can be their own lawyer and successfully defend himself or herself in court. In reality, even professional programmers, blockchain specialists who tried to use smart contracts for the first time, made a mistake when creating The DAO investment consortium. The mistake of ambiguity in code execution cost $ 60 million [25]. Education, even in the broadest sense, is unlikely to promote the technology to the masses.

Can an initially experimental, not claiming universality technology become mass? Declaring anonymity and decentralization as the basic properties, Bitcoin was a private solution to the purely ideological problem of crypto-anarchism. This is a radical trend of the libertarian ideology, which for a long time has studied the possibility of the existence of non-governmental payment and monetary systems with private emission centers [26]. At the same time, people have had no payment problems since the sixth century BC, after cash was invented. It is not surprising that, being an ideological product, cryptocurrency as money with its high volatility turned out to be quite doubtful [27].

MAIN PROBLEMS OF CURRENT BLOCKCHAIN INTRODUCTION

Besides high volatility, the problems of the technology are slow transaction speed, high energy consumption, poor scalability [28, 29]. Indeed, in 2018, Bitcoin consumed 47 Tw/hour, which is twice as much as Ireland's electrical consumption. Bitcoin transaction speed is about 7 t/sec, and the average waiting time of transaction confirmation is 55 minutes. To compare, the Visa payment system processes 24,000 t/sec, and the average waiting time is 3 seconds. It is hardly possible to overcome these problems while maintaining blockchain's decentralization and openness, since the only practical method that provides these properties is the energy-consuming Po W. Therefore, the appeal to blockchain's high speed is a bold claim. In the United States, it might be considered fast regarding the processing of payment checks, which still account for 25% of retail payments there[8], because the US national clearing system NACHA ACH accepted same day payments only in 2016.

Given the above problems, one can doubt the declared cost savings when implementing blockchain [30]. Consulting firms tout cost savings of 70% for systems and infrastructure. They do this in the context of general digitalization, modernization and abandoning obsolete systems, which will obviously reduce costs regardless of distributed ledgers. The data storage in a distributed ledger is expensive even at relatively high corporate prices for classic databases. Moving to the "free" IBM Hyperledger will cost a mid-sized enterprise about $ 140,000[9], not including implementation costs.

THE PROBLEM OF TRUST IN SYSTEMS WITH NO TRUSTED PARTY

Finally, the most ironic factor, which is a brake for the technology penetration. A study conducted by PwC consultants showed that the main limiting factor in implementing blockchain is the lack of trust [31]! The world does

[8] According to the data by creditcards.com. URL: https://www.creditcards.com/credit-card-news/payment-method-statistics-1276.php (accessed on 10.10.2019).

[9] According to the data by EY, Total cost ownership for blockchain solutions. 2019; Apr. URL: https://www.ey.com/Publication/vwLUAssets/ey-total-cost-of-ownership-for-blockchain-solutions/$File/ey-total-cost-of-ownership-for-blockchain-solutions.pdf (accessed on 10.10.2019).

not trust the technology with the "inbuilt trust". That makes sense. From a philosophical point of view, a consensus indeed is not trust. Consensus decisions can be arbitrarily wrong and unfair. Moreover, the genesis of the technology comes from the ideology by radical revolutionaries who want to rebuild the world and destroy modern capitalism. Can we trust the anonymous majority of greedy anarchists? Neither government institutions nor the corporate world trust technology, aiming to destroy the modern world.

It is getting more interesting when it comes to exclusive blockchains. The very fact of creating private exclusive blockchains means distrust to public blockchains, with trust in the technology. Trust in established institutions is always higher than in an anonymous crowd. However, if we trust an imaginary IBM and its affiliates, the questions arise: why do we need a significantly more expensive and limited distributed ledger? why not just put your data in the cloud of a trusted company and assign a trusted company a cryptographic certificate service provider? This solution will definitely be faster and costs are better forecasted. If there is no trust, how can we participate in a proprietary distributed ledger that ensures trust by the participation of a party we do not trust?

The US Senate hearings on Facebook's plans to introduce Libra cryptocurrency are quite indicative. "I don't trust you guys," said Senator Martha McSally (R-Arizona) to Facebook representative David Marcus[10]. Trust is fragile; in this regard, even the flagship of the national economy cannot expect special treatment.

To summarize, blockchain actually:

- is not a "new Internet";
- is likely to provide a consensus, not trust;
- popular consensus algorithms have drawbacks allowing attackers to take advantage;
- does not provide equal participation;
- is not a database and does not provide immutable data storage.

[10] Quoted from: Katz M. The U.S. Senate really doesn't like Facebook's Libra cryptocurrency plans // digitaltrends.com, 2019;16 Jul. URL: https://www.digitaltrends.com/news/senate-facebook-libra-hearing-david-marcus/ (accessed on 10.10.2019).

ANONYMOUS AND FREE BLOCKCHAIN

Is it possible that blockchain is really anonymous and free? In general, no and no. Most systems based on blockchain, e.g. Bitcoin, are pseudo anonymous. The fact that the crypto wallet is not linked to the personal data does not make the system "anonymous". Even with anonymizers and the Tor network, real users can be detected by metadata with a very high degree of confidence both by special services and by private specialists. In the case of illegal activities, blockchain's complete transparency provides justice with cogent evidence [32].

Free blockchain is also just a declaration. There are more than 1,000 patents for distributed ledgers registered in the USA[11]. It is unlikely that leading financial and technology companies patent the technology for altruistic reasons. Even "free" technologies are a source of profit for such companies. There are corporate wars for control over the technological context even in the field of open source ledgers, for example, between Intel and IBM to control Hyperledger.

BLOCKCHAIN AND TRADITIONAL INSTITUTIONS

Despite the fact that blockchain's only significant use is cryptocurrencies, they do not shake the authority of classic financial institutions. Traditional banks with traditional trust in the financial system of the traditional state are still better in every aspect[12]. Attempts to implement distributed ledger technologies in the traditional financial sector, as elsewhere, have naturally been unsuccessful: contrary to expectations, the technology in no way reduces IT infrastructure costs, cost of interbank payments or speeds up transactions. The advantages of blockchain such as smart

[11] According to the data by bitcoinmarketjournal.com. URL: https://www.bitcoinmarketjournal.com/blockchain-patents/ (accessed on 10.10.2019).

[12] According to the Edelman Trust Barometer, in 2019, trust in banks /blockchain /cryptocurrencies on average among the entire population of the Earth, was respectively: 61 (trust) / 55 (neutral ratio) / 35 (distrust). URL: https://www.edelman.com/trust-barometer (accessed on 10.10.2019).

contracts, encryption, and distributed ledger are separate concepts. The three are independent of blockchain, they do not need to be implemented together in the IT infrastructure of financial organizations [33]. This is probably why Ripple, the most successful company declaring "interbank payments on blockchain", turned out to use traditional instruments for interbank payments, not blockchain[13].

Regulatory measures in banking and financial market are to protect investors. This is not "greed", but the result of the long development of state institutions.

No blockchain will replace or strengthen the institution of democratic elections. A blockchain voting system is not protected from "stuffing", similar to traditional ballot boxes. How can blockchain help if a potential candidate is simply not allowed to have a democratic will?

A blockchain logistics system is the same as any system — it is "garbage in, garbage out". For example, in 2006, Walmart launched a system to track its fruit from producer to buyer. In 2009, they abandoned it, and in 2017, they re-launched it on blockchain [34]. In 2006, the main problem of the system was that the manufacturers did not want to enter the data. Obviously, blockchain implementation did not solve the problem. The problem of food labeling can easily be solved by traditional means, for example, by the Russian EGAIS and Mercury systems.

CONCLUSIONS

In conclusion, it is worth noting that the social and cultural aspects of hype around blockchain are extremely interesting. How has blockchain mania embraced serious business? How did a social order come about on blockchain? How did an experimental technological solution generate a virtually sectarian belief system with features of a destructive cult?[14] Future researchers have yet to answer these questions, but now there is reason to believe that blockchain is more a social phenomenon [35] than a rational one [36].

Blockchain and distributed ledgers are not a foundational technology. In general, they do not have the properties of the immutable data storage, trust, anonymity, low transaction and adoption costs. All current consensus technologies have fundamental flaws. Cryptocurrency technology is original, but it was a private experimental solution to a specific ideological problem of the libertarian political agenda. Consensus does not provide trust. Delayed blockchain adoption, in particular in traditional financial institutions, is natural, since the technology does not show better results than current digital solutions. Traditional economic institutions have greater public trust. Significant investment in blockchain and distributed ledgers are unlikely to pay off soon. De facto, they guarantee further search for application of the technology in various fields of human activity, including the financial sector.

[13] According to the data by Financial Times: Kelly J. Blockchain insiders tell us why we don't need blockchain. 2018; May 2. URL: https://ftalphaville.ft.com/2018/05/02/1525253799000/Blockchain-insiders-tell-us-why-we-don-t-need-blockchain/ (accessed on 10.10.2019).

[14] In May 2018, the entrepreneur launched a religious cult based on blockchain called "0xΩ". URL: https://www.americamagazine.org/politics-society/2019/06/14/can-technology-behind-bitcoin-be-used-build-belief-system (accessed on 10.10.2019).

REFERENCES

1. Autore D.M., Clarke N., Jiang D. Bitcoin speculation or value creation? Corporate Blockchain investments and stock market reactions. *SSRN Electronic Journal*. 2019. DOI: 10.2139/ssrn.3385162
2. Tapscott D., Tapscott A. Blockchain revolution: How the technology behind Bitcoin and other cryptocurrencies is changing the world. New York: Portfolio; 2018. 432 p.
3. Swan M. Blockchain: Blueprint for a new economy. Sebastopol, CA: O'Reilly Media, Inc.; 2015. 152 p.
4. Mougayar W. The business Blockchain: Promise, practice, and application of the next Internet technology. Hoboken, NJ: John Wiley & Sons, Inc.; 2016. 209 p.
5. Fanning K., Centers D.P. Blockchain and its coming impact on financial services. *The Journal of Corporate Accounting & Finance*. 2016;27(5):53–57. DOI: 10.1002/jcaf.22179

6. Hassani H., Huang X., Silva E. Banking with Blockchain-ed big data. *Journal of Management Analytics*. 2018;5(4):256–275. DOI: 0.1080/23270012.2018.1528900
7. Iansiti M., Lakhani K.R. The truth about Blockchain. *Harvard Business Review*. 2017;95(1):118–127. URL: https://enterprisersproject.com/sites/default/files/the_truth_about_blockchain.pdf
8. McGrath R.G. The pace of technology adoption is speeding up. *Harvard Business Review*. 2013;(Nov.). URL: https://hbr.org/2013/11/the-pace-of-technology-adoption-is-speeding-up
9. Rogers E.M. Diffusion of innovations. 3rd ed. New York, London: The Free Press; 1983.
10. Woodside J.M., Augustine F.K. Jr., Giberson W. Blockchain technology adoption status and strategies. *Journal of International Technology and Information Management*. 2017;26(2). URL: http://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1300&context=jitim (accessed on 10.10.2019).
11. Stratopoulos T.C., Wang V.X. Blockchain technology adoption. *SSRN Electronic Journal*. 2018. DOI: 10.2139/ssrn.3188470
12. Ahuja G., Lampert C.M. Entrepreneurship in the large corporation: A longitudinal study of how established firms create breakthrough invention. *Strategic Management Journal*. 2001;22(6–7):521–543. DOI: 10.1002/smj.176
13. Lamport L., Shostak R., Pease M. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*. 1982;4(3):382–401. DOI: 10.1145/357172.357176
14. Fischer M., Lynch N., Paterson M. Impossibility of distributed consensus with one faulty process. *Journal of the ACM*. 1985;32(2):374–382. DOI: 10.1145/3149.214121
15. Ben-Or M., Hassidim A. Fast quantum Byzantine agreement. In: STOC'05. Proc. 37th Annu. ACM symp. on theory of computing (Baltimore, MD, May 22–24, 2005). New York: ACM; 2005:481–485. DOI: 10.1145/1060590.1060662
16. Krawisz D. The proof-of-work concept. Satoshi Nakamoto Institute. 2013. URL: https://nakamotoinstitute.org/mempool/the-proof-of-work-concept/ (accessed on 10.10.2019).
17. Bissias G., Levine B.N., Ozisik A.P., Andresen G. An analysis of attacks on Blockchain consensus. URL: https://arxiv.org/pdf/1610.07985.pdf (accessed on 10.10.2019).
18. Zhang S., Lee J.-H. Double-spending with a Sybil attack in the Bitcoin decentralized network. *IEEE Transactions on Industrial Informatics*. 2019;15(10):5715–5722. DOI: 10.1109/TII.2019.2921566
19. Demeester T. Critique of Buterin's "A proof of stake design philosophy". Medium. 2017. URL: https://medium.com/@tuurdemeester/critique-of-buterins-a-proof-of-stakedesign-philosophy-49fc9ebb36c6 (accessed on 10.10.2019).
20. Zhang S., Lee J.-H. Analysis of the main consensus protocols of Blockchain. *ICT Express*. 2019;5(3). DOI: 10.1016/j.icte.2019.08.001
21. Wahab A., Memood W. Survey of consensus protocols. 2018. URL: https://arxiv.org/ftp/arxiv/papers/1810/1810.03357.pdf (accessed on 10.10.2019).
22. Grewal-Carr V., Marshall S. Blockchain: Enigma. Paradox. Opportunity. Deloitte. 2016. URL: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf (accessed on 10.10.2019).
23. Stolfi J. Letter to the Editor, NIST Reports. Ref: NISTIR 8202 (DRAFT): Blockchain Technology Overview. 2018. URL: https://www.ic.unicamp.br/~stolfi/temp/nist-report-review.pdf (accessed on 10.10.2019).
24. Radoccia S. What's holding Blockchain back from large-scale adoption? Forbes. Sept. 21, 2017. URL: https://www.forbes.com/sites/quora/2017/09/21/whats-holding-blockchain-back-from-large-scale-adoption (accessed on 10.10.2019).
25. Castillo M. The DAO attacked: Code issue leads to $ 60 million ether theft. Coindesk. June 18, 2016. URL: https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theft (accessed on 10.10.2019).
26. Karlstrøm H. Do libertarians dream of electric coins? The material embeddedness of Bitcoin. *Distinktion: Scandinavian Journal of Social Theory*. 2016;15(1):23–36. DOI: 10.1080/1600910x.2013.870083

27. Krylov G.O., Lisitsyn A.Y., Polyakov L.I. Comparative analysis of volatility of cryptocurrencies and fiat money. *Finansy: teoriya i praktika = Finance: Theory and Practice.* 2018; 22(2):66–89. (In Russ.). DOI: 10.26794/2587–5671–2018–22–2–66–89
28. Goswami S. Scalability analysis of Blockchains through Blockchain simulation. UNLV Theses, Dissertations, Professional Papers, and Capstones. 2017;(2976). URL: https://pdfs.semanticscholar.org/108f/9d7493fecd7cdb1a2a123d89a4db16b79679.pdf?_ga=2.210275989.1023187009.1572354254–1709531060.1571930732 (accessed on 10.10.2019).
29. Truby J. Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. *Energy Research & Social Science.* 2018;44:399–410. DOI: 10.1016/j.erss.2018.06.009
30. Bloomberg J. Don't let Blockchain cost savings hype fool you. Forbes. Feb. 24, 2018. URL: https://www.forbes.com/sites/jasonbloomberg/2018/02/24/dont-let-blockchain-cost-savings-hype-fool-you/#3b47f4f45811 (accessed on 10.10.2019).
31. Davis S. Likens S. Blockchain is here. What's your next move? Pw C. 2018. URL: https://www.pwc.com/gx/en/issues/blockchain/blockchain-in-business.html (accessed on 10.10.2019).
32. Bohannon J. Why criminals can't hide behind Bitcoin. Science. March 09, 2016. DOI: 10.1126/science.aaf4167
33. Halaburda H. Blockchain revolution without the Blockchain? *Communications of the ACM*. 2018;61(7):27–29. DOI: 10.1145/3225619
34. Stinchcombe K. Blockchain is not only crappy technology but a bad vision for the future. Medium. Apr. 5, 2018. URL: https://medium.com/@kaistinchcombe/decentralized-and-trustless-crypto-paradise-is-actually-amedieval-hellhole-c1ca122efdec (accessed on 10.10.2019).
35. Albrecht S., Lutz B., Neumann D. How sentiment impacts the success of Blockchain startups. An analysis of social media data and initial coin offerings. In: Proc. 52nd Hawaii int. conf. on system sciences. 2019:4545–4554. URL: https://scholarspace.manoa.hawaii.edu/bitstream/10125/59892/ 0452.pdf (accessed on 10.10.2019).
36. Lee C.C., Kriscenski J.C., Lim H.S. An empirical study of behavioral intention to use Blockchain technology. *Journal of International Business Disciplines.* 2019;14(1):1–21. URL: https://faculty.utrgv.edu/louis.falk/jibd/JIBDmay19.pdf (accessed on 10.10.2019).

ABOUT THE AUTHORS

Grigorii O. Krylov — Dr. Sci. (Phys.-Math.), Cand. Sci. (Engin.), Cand. Sci. (Juris.), Professor, Department of Information Security, Financial University, Moscow, Russia;
Professor at National Research Nuclear University MEPhI, Honorary Figure of Russian Higher Education, Moscow, Russia
nik155@yandex.ru

Vladimir M. Seleznev — Cand. Sci. (Engin.), MBM, Member of the Board, JSC LatCard (Electronic money financial institution), Riga, Latvia
v_seleznev@pisem.net

The article was submitted on 02.09.2019; revised on 11.09.2019 and accepted for publication on 20.10.2019. The authors read and approved the final version of the manuscript.