The Main Limitations of Applying Blockchain Technology in the Field of Education

Naumova O.A.
Samara State University of Economics
Samara, Russia
e-mail: naumovaoa@gmail.com

Naumov D.V.
IndaJava company
Samara, Russia
e-mail: naumovdv@gmail.com

Svetkina I.A.
Samara State University of Economics
Samara, Russia
e-mail: svetkinairina@yandex.ru

***Abstract*—The article identifies the main features of the application of blockchain technology, which caused a lot of positive feedback in scientific circles and professional communities. After success in the financial market, where the blockchain contains blocks that are iced in the chain, which describes absolutely all transactions with virtual coins (such as Bitcoin, Litecoin, Ethereum and others), there were prospects for evaluating the possibility of its successful application in other areas.**

Considering that the sphere of education in Russia is going through a period of reforms, special attention is paid to the opportunities and problems of application in this sphere.

The article discusses the effectiveness of the application of blockchain technology for the distributed registry and for mass application in the field of education. And also an estimation of the probability of the possibility of improving the educational process. The analysis of the advantages of the technology that allowed it to successfully spread its crypto currency in the market of anonymous transactions and their application in the subject field of education, in comparison with classical technologies, with the central node-regulator, for example, the client-server.

Keywords—blockchain technology, education, hashing, client/server systems.

I. INTRODUCTION

The recent development and introduction of blockchain technology received many positive reviews in both scientific and professional sectors. The technology has been termed "Distributed ledger technology" (abbreviated to DLT). Since the successful launch of cryptocurrencies [2] (Bitcoin, Litecoin, Ethereum, among others), where blockchain is used as a mechanism for value transferring, many experts believe that this technology is poised to be introduced in many other industries, one of these being in the field of education [10,11,12,13]. However, a lot of the early reviews of the technology's applications were made based on high-level analysis without necessarily focusing on important details which could be obstacles for its further expansion in the field of education.

II. DISCUSSION

The recently introduced Federal Education Standard 3+ and Federal law "Education in Russian Federation" prescribe new scope, models and technologies for application in education. Chapter 7 of Federal Education Standard 3+ defines the transition into a digitalized form of education, which becomes an essential part of the digital economy (Putin, 2017; The institute for economic strategies, 2017[3]). New developments and technologies were taken into consideration by many professionals in the educational sphere and many studies based on the blockchain technology have been produced. Consequently a number of new research and articles concerning the application of decentralized public ledgers appeared in the academic literature:

- Academic periodical «Fundamentalnie issledovania»[Fundamental research] ISSN 1812-7339 (2017, №9)
- INTERNATIONAL JOURNAL OF OPEN INFORMATION TECHNOLOGIES ISSN: 2307-8162 (2017, №12)
- Eco-potential ISSN: 2310-2888 (2017, №2)
- Professional Education. Stoliza ISSN: 1999-2262 (2017, №4)
- Problematic of management - 2017 25-я Russian student's conference. FGBOYVO «GYY» 2017
- Scientific-practical conference "New information technologies in Education and Science" 2017
- XIII International scientific-practical conference "Modern instrumental systems, IT technologies and innovations", 2018

III. RESEARCH METHODS

To understand all possible advantages of the blockchain technology that's been addressed by many authors, we first

978-1-7281-1931-1/19/$31.00 ©2019 IEEE

need to analyze DLT in more detail. The analysis will focus on the blockchain technology that can be found in Bitcoin. There are also other variations of blockchain technology that's being used, although these are all based on the same overarching principles.

Blockchain is a technology which records and stores information and transactions on a decentralised database and comprises a network of interlinked computers which uses cryptography to secure exchanges. In this decentralised database, all information is located in the form of blocks [1].

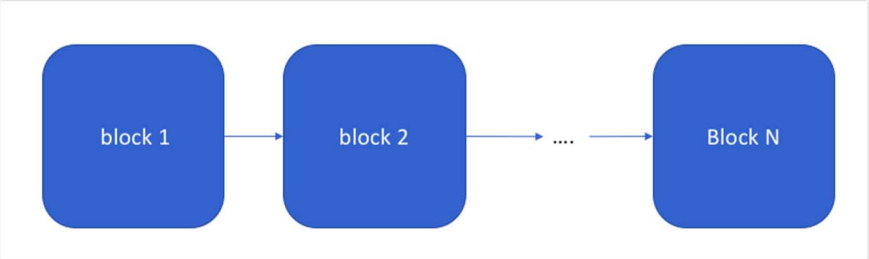

Fig. 1. Illustration of workflow in a blockchain.

Each block can contain specific information or a set of several data at once, as well as information about the previous block. This is not the entire contents of the previous block and not its identifier, but the result of a unidirectional hash function from the contents of the previous block (Figure 1). Hashing [8] is the transformation of an array of input data with a given length into a (output) string of the specified length, all performed by executing an algorithm. A function that embodies the algorithm and performs the transformation is called a "hash function" or "fold function". The input data is called the input array, the result of the conversion (output data) is called a "hash". Blockchain uses unidirectional networks, the result of which does not allow you to restore the contents. Thus, the information in the previous block remains only known to its block and data is effectively travelling in one direction. The new block will always be added only to the end of the chain and refer to the previous one. It is not possible to delete a block from the chain as this would imply that the next block will no longer refer to the previous block and the circuit will be broken.

The calculation of the hashes and the preparation of blocks for insertion into the chain is occupied by all nodes of the blockchain network. If the majority of participants in the blockchain network obtain the same result, the block will be added while the remaining nodes will be ignored. To test the result, the previous blocks are also recalculated to avoid the insertion of compromised data.

This reveals the first of the problematic areas with the technology - the redundancy of the calculations. There is a misconception that distributed nodes in the blockchain network are involved in distributed calculations. In fact, all nodes in parallel calculate the same thing. As a result, half of the nodes do this without any meaningful result, while the remaining half checks already performed operations by other members in the blockchain network.

For a blockchain network to exist and remain functional, you need a large number of nodes in it. By increasing the number of network members you improve its resistance to compromised or modified data and reduce the chance of errors occurring. This leads to another disadvantage with the distributed architecture of the blockchain - the motivation of the participants. The question arises, how do you motivate participants to join the network and allow their resources to produce redundant calculations as described above?

In the blockchain of the Bitcoin crypto currency network, participants whose calculations were successful and contributed to obtaining the expected result, receive incentives through gratification in the given cryptocurrency for their use of use of time and processing power. However, the number of Bitcoin coins is finite with a diminishing marginal return, meaning that in the foreseeable future such payments will no longer be possible. If there is no change in the way participants are rewarded for their participation in the blockchain network, this may eventually lead to the end of the Bitcoin.

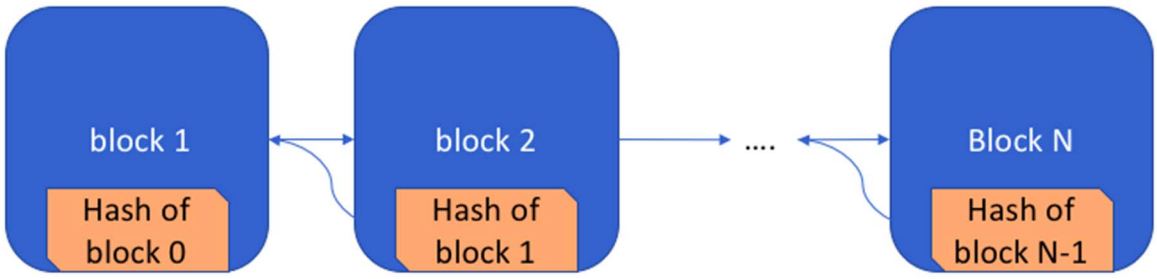

Fig. 2. A blockchain process.

978-1-7281-1931-1/19/$31.00 ©2019 IEEE

IV. The Results

Let's analyze a hypothetical blockchain made up of Russia's universities, containing information for storage and verification of diplomas, certificates and other documents confirming any educational qualification or achievement. As of 2017 there were 1,256 universities registered in Russia. To set up the blockchain network we would need to:

• allocate computing power for the calculation of blocks and their verification;

• provide communication channels for replicating the results, as well as receiving the results of other network participants;

• agree to disclose information about all certificates, diplomas and other documents, which will comprise all the information stored in the network. One of the main ideas behind blockchain imply full, non-interrupted accessibility of data to all network participants.

This will lead to increased costs for universities and necessitate amendments to the educational legislature. Since the network is decentralized it may face another difficulty relating to aligning the interests of all participants. Consider the same network from the example above. Let's assume that some of the participants do not want to spend resources on calculating "foreign" data and become only consumers in the network, not contributing to verifying and solving algorithms. Such a scenario will result not so much in increasing the burden on the resources of other participants, but rather in undermining the reliability of the network.

In fact, this is equivalent to alleviating the network of this node. As mentioned earlier, a blockchain network is possible only if there are enough participants in it. The fewer participants there are in the network, the higher the chance of compromised data appearing in it. The scenario may be different - all network members conscientiously perform calculations, but a dominant group of nodes appears whose computing power provides it with 50% or more of its computational requirements. In this case, the dominant group may intend to calculate data in which it is interested, ignoring the interests and data of the other network members. For the Bitcoin network, this option is also possible, but is complicated because of the very large number of participants. However, it remains a likely outcome, especially in smaller networks.

Separately, you can use the protocol from the network. All participants work under one agreed protocol. If a member appears on the network and changes the protocol, the others can ignore or agree with it. On March 11, 2013 [9] version 0.8 of Bitcoin blocks had such an instance of a change in protocol. A significant part of the network did not agree with the new protocol, and it was not applied to the entire network. A scenario is also possible when the dominant group intends to introduce changes in the protocol and, as in the case of monitoring more than 50% of the computing power of the network, will force the data to change for all other participants.

The next feature of the blockchain network is the complete anonymity of the participants. As a result, the appearance of nodes in the network, whose activities will be unchecked, is not ruled out. In the case of the example network of universities, a node may appear in it, which will begin to fill the chain of blocks with its data. Certificates of professional development given by a fictional educational institution might be such an example. Even though this institution might not be registered as an educational institution, its data can still be accepted and will be forever in the chain.

It would seem that the solution to the shortcomings described above can be carried out by a supervisory authority or a centralized node that would provide control in the network. But this of course contradicts the technology of the distributed registry in the blockchain [1,14]. And, as a consequence, applications of blockchain technology can be made obsolete. A more preferable solution would be to revert to the more traditional peer-to-peer server-client model where the server manages and controls customer data.

V. Conclusion

Our research showed that currently blockchain technology for distributed ledger is not efficient in education and it's highly unlikely it could improve the education process. All advantages of the technology applied in anonymous crypto currency transactions are not easily applicable in the field of education. Ultimately it adds a lot of complexity to the network and generally blockchain cannot compete with more conventional technologies such as client/server systems where information is stored centrally.

References

[1] C. Raval, "Decentralized apps. Blockchain technology" [Dezentralizovannie prilogenia. Technologia Blockchain v deistvii], ISBN: 978-5-496-02988-9.

[2] D. Tapscott, A. Tapscott, "Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money", Business, and the World ISBN: 9780241237854.

[3] V.V. Putin, St Petersburg International Economic Forum June 2 2017, [Video], URL: http://kremlin.ru/misc/54667/videos/3509.

[4] A. Grech, A.F. Camilleri, "Blockchain in education", Report by the Joint Research Centre (JRC), the European Commission's science and knowledge service, 2017.

[5] A. Solovev, "Underwater stones of Blockchain" [Blockchain: Podvodnie kamni], Open Systems/SUBD, 2016, no. 4, URL: http://www.osp.ru/os/2016/04/13050987/.

[6] A.V. Klechikov, M.M. Pryanikov, A.V. Chugunov, "BlockchainTechnologies and their Application in Government Administration", International Journal of Open Information Technologies ISSN: 2307-8162, vol. 5, no. 12, 2017.

[7] A. Fedonov, R. Fedonov, "The use of energy saving technologies in the production activity of industrial enterprises".

[8] C.C. Chagin, "Blockcain for dummies(straightforward issues about tmplementing Blockcain in education)" [Blockchain dlya chainikov (otkrovenno o zadachah vnedrenia technologii Blockchain v obrazovanii)], Professionalnoe obrazovanie. Stoliza, Academic professional press, Moscow, ISSN: 1999-2262.

[9] A.V. Frolov, "Prospective of Blockchain technology in Education" [Perspectivi primenenia technologii Blockchain v sphere obrazovania], XIII International scientific-practical conference "Modern instrumental systems, IT technologies and innovations", 2018.

[10] D.A. Bogdanova, "New technologies for Education. New IT technologies in Education and Science" [O novih technologiyah dly

obrazovania. Novie informazionnie technologii v obrazovanii i nayke], Article from X International scientific – practical conference 2017.

[11] D.C. Yarzev, "Blockchain in Education. Applying prospective. Management problematics" [Blockcain v Obrazovanii: Perspectivi primenenia. Problemi ypravlenia], article from 25 Russian students conference FGOYBO "GYY", 2017.

[12] A. Pazaitis, P. de Filippi, V. Kostakis, "Blockchain and value systems in the sharing economy": The illustrative case of Backfeed, vol. 125, December 2017, pp. 105-115.

[13] H. Malviya, "How Blockchain will Defend IOT, 2016", URL: https://ssrn.com/abstract=2883711, (Accessed 1 February 2018).

978-1-7281-1931-1/19/$31.00 ©2019 IEEE