Theory Game as Priority Area of Researches for Development of Blockchain Technology

Saltykov S.A., Rusyaeva E.Yu.
V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences
Moscow, Russia
rusyaeva@ipu.ru, ssaltykov@mail.ru

***Abstract*—It is shown that game theory with imperfect information «cover» the most of the deep challenges facing blockchain technology. Various challenges of this technology are analyzed and allocated main of them. For each of critical challenges, it considered in what measure the answer to him connected with the need of creation of new scientific results for some sections of game theory. The conclusion is drawn that an essential part of the deep challenges of a blockchain it is possible to reduce to a game-theoretic design of a situation of multiagency interaction. In this case, the consensus of users a blockchain system concerning the reliability of any transaction established.**

Keywords— blockchain; distributed registers; theory game; establishment of consensus; decentralization; scalability; multiagent systems

I. INTRODUCTION

In this article, we will consider prospects and abilities to integrate one of the types of the distributed ledgers, blockchain technology, with some directions of game theory for their mutual development. In the analysis of the international researches on this subject before us, there were some questions.

On the one hand, in some works, it is said [1, 2] that the blockchain represents a synthesis of cryptography and game theory. That is, authors of these researches consider that if to allocate two the components which are most significantly characterizing a blockchain, then the game theory will appear among them. Then it turns out that the game theory role in creation and development of a blockchain is enormous.

On the other hand, there is a number of the scientific works leading including, among the researches of the general, survey character in service Google Academy devoted to blockchain technology in general and the challenges facing this technology. The role of game theory isn't mentioned in them in general [3, 4] or discussed only casually [2].

Thus, it is possible to conclude that at the moment at a blockchain community there is no consensus opinion on a game theory role in a blockchain. But what true situation? Perhaps, specialists in a operations research it intends lobby a game theory role to give weight to the studies, and real practice of a blockchain perfectly does without game-theoretic constructions? Or all on the contrary, and the blockchain industry desperately needs the breakthrough ideas in game theory? These breaks can become the guarantee of further successful strategic development a blockchain industry, but still ordinary it is challenging to realize blockchain programmers as the problem roots too deeply? What detailed description of the essence of why the role of game theory is high? The blockchain industry needs all game theory in general or its some concrete sections and why?

We will try to give answers to these questions in our research. We consider that for this purpose it is necessary for details, without abstracting from concrete technical information, to analyze the profound challenges standing before a blockchain industry. Further, it is required to show, how correctly the game theory in what measure it helps to answer it`s connected with the answer to each of separate challenges.

Once again we will emphasize that the understanding of technical nuances even, at least, at the primary level, is necessary for the analysis here: without them, it is possible to miss the most important. The "flat," reductive picture can give the incorrect answer about a game theory role.

Therefore in this article, we will pay special attention to essentially important technical details a blockchain industry. We consider that such detailed justifications so far in literature aren't enough. For example, in work where there is a review of challenges [3], aren't distinguished main from them, and connection of challenges with game theory isn't specified in general. In other papers, there is the thesis about the connection between game theory and a blockchain [2] but isn't proved at what measure it is present.

Besides, it is indicated the connection between blockchain and game theory out of a context of all standing challenges before the industry. Such a thesis looks taken out of a context, and from it, game theory role "proportions" aren't clear.

To avoid these things, we will try to stretch a complete thread from those external conditions in which there is a blockchain industry, and its internal contradictions, the dynamic of its development, to a real role of new results in game theory in the strategic development of a blockchain industry.

Thus, we will define whether researches on game theory (and according to what her sections) are a priority for development of such important element of digital economy as the distributed ledger in general and a blockchain in particular.

978-1-5386-4924-4/18/$31.00 ©2018 IEEE

II. BLOCKCHAIN AND GAME THEORY: ABILITIES TO INTEGRATE

To resolve the problem of "blockage," or rupture of a cycle at certain points, the matrix of distribution resources can be used. P-direction (vertical) of the matrix stands for the list of all research scopes having Higher Attestation Commission passports. It contains about 5 thousand names. This quantity approximately corresponds to the number of research laboratories in our country. The other axis – N (horizontal) – measures the stages of the life cycle of innovations formulated by proprietary typology [1,2]. So, as a result, we will receive the following columns: 1) fundamentally searching, 2) oriented radically, 3) declaratively applied, 4) conditionally applied with an endless commercialization potential and 5) provisionally applied with high commercialization potential. On the whole, we receive the matrix of 5 thousand lines and five columns containing 25 thousand cells.

Further, the topics of research works of all laboratories in the country are analyzed, which is about 7-10 thousand. The task is to divide the 10 thousand questions between 25 thousand "sections." For this distribution, it is necessary to identify each value at matrix axes.

We will assume that it is possible to refer topics of laboratory researches to a specific area of research scopes from the Higher Attestation Commission passport. Thus it becomes possible to define a "line" to place the topic of a laboratory. The second step is to define the "column" in the matrix, for what the author's method used.

III. INNOVATIVE CYCLE STAGE IDENTIFICATION METHOD FOR SUBJECTS OF SCIENTIFIC LABORATORIES RESEARCHES

According to Vitalik Buterin, the creator of the Ethereum platform, now the blockchain faces three main challenges: scalability, safety and privacy [3].

We will show that problems with scalability in many aspects result from the need for interoperability of blockchains and imperfections of the most often applied way of verification of transactions – Proof-of-work. In turn, questions about the safety of blockchains are also in many aspects caused by this way of confirmation of operations: it is the reason that lies on a surface and often discussed. These are threats of centralization of a blockchain and, as a result, copying of its transactions, the attacks "double spending," etc.

That is, in this section, we will prove that if to look narrowly at details, challenge of scalability and safety closely connected among themselves. Also, they are in many respects determined by the need of the solution of questions of the interaction of blockchains with each other and design of new, more perfect ways of verification of transactions in a blockchain [3].

We will in detail consider two "well-known" challenges, scalability and safety, and "deep" challenges lying behind them.

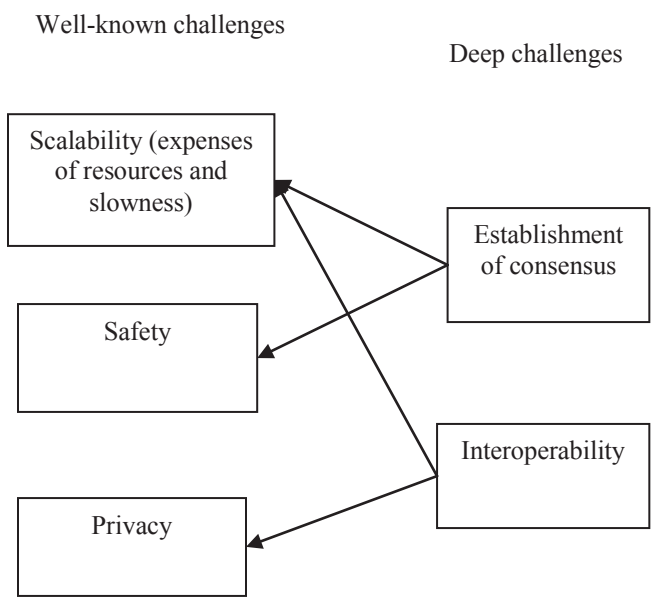

Fig. 1. Challenges for a blockchain

A. Challenges Scalability. Expenses of resources

We will consider a scalability challenge. Now transactions often are confirmed too long. The total number of transactions which can be written down in a blockchain in the unit of time isn't enough so that millions of users used this actual blockchain. Also, electric power costs of mining (production) of blocks of a chain of transactions are at the moment unfairly big.

If to try an essential part of processes of life of society as it is often told in advertising slogans, "to transfer to a blockchain," then the blockchain platform won't be able to function. Transactions will be carried out unacceptably slowly, the waiting list for verification of transactions will quickly grow, and they are carrying out commissions will be unacceptably high. Besides, expenses of the electric power will be just disproportionate to the public benefit brought by such blockchain. Already now, for example, the network of bitcoin consumes more electric power, than some countries. And this with the fact that the bitcoin hasn't managed to become the standard blockchain platform not only yet, but also even adequate means of implementation of payments.

In what one of the main reasons for these problems? It is in many respects in the most often used way of verification of transactions – Proof-of-Work ("the proof of work").

Initially, the idea of the proof of work as the way of the choice of the miner was breakthrough and very effectively worked in the network of bitcoin. But approximately in a decade mining has rested against the technologically caused ceiling. With the growth of computing power of network complexity of a task of selection of a hash everything increases (as it is necessary to select a smaller hash), and energy consumption grows. To cover this cost, miners increase the commissions of transactions, and at the smaller commissions, the money transfer can go several days and more.

Besides, because of growth of computing complexity of mining, it isn't favorable to ordinary users of personal computers to participate in drilling anymore, and he is carried out now by some of the huge pools (associations) of miners. And it leads to the threat of centralization of a network with all that it implies.

On a twist of fate, the mining which is thought up avoiding centralization and has brought to it, eventually. In this aspect, it becomes clear that "cosmetic" changes like increase in the size of the block and removing of information to a part out of limits of a blockchain won't solve a problem as it roots like mining.

What can be the adequate answer to such challenges? We will consider him below; for now, we continue consideration of a challenge of scalability.

B. Challenge scalability. Interoperability

Another aspect of problems of scalability is connected about Interoperability of blockchains, that is, with a possibility of their effective interaction. Here the question is raised so: or there will be a one, and the only blockchain which has won a competition and became a blockchain platform by default for digitalization of all aspects of life or there will be a big set of blockchains of different function between which it is necessary to carry out interaction.

Both common sense and experience of the IT industry prompt that one blockchain for all and all are from the area of a fantasy: on the Internet, there is too no fact that the only website, but also even completely dominating company. Therefore, sooner or later different blockchains should "communicate" with each other. And this necessary condition for successful scaling.

C. Challenge safety

We will pass to safety challenges. The main danger to a blockchain consisted of a possibility of his capture by malefactors and considered that it is easier to occupy the centralized network than decentralized. The fact that the danger of centralization results from the nature of mining has shown above. Moreover, if we eliminate this vulnerability, and we will change a way of verification of transactions to "the proof of a share" (more detailed it will be considered below), then one security concerns will be replaced with others: when using Proof-of-Stake the network is subject to the attack "nothing on stake". That is, the wrong choice not only the way of verification of transactions but also even his parameters will be a severe threat to security. Therefore the conclusion of the safety of blockchain platforms to a new level is in many respects caused by designing of an effective way of verification of transactions.

Thus, two "deep" challenges which we will consider further are need of ensuring interoperability of blockchains and designing of more effective of ways of verification of transactions.

IV. Answers to profound challenges of a blockchain

In general and a possibility of interoperability of a blockchain, in particular, the technology of a sharding which consists in the organization of work of a hierarchically ordered set of blockchains of different type and the appointment can provide the need for scalability. At the same time in such a hierarchy, there is a root blockchain.

The idea and the prospect of the development of a sharding are that here the structure of many social institutes of society is copied. The root blockchain plays a role of the court in this analogy, and affiliated blockchains contain information on operating activities.

We see that during natural development of architecture in blockchain technology delegation and multinumber of stories appear; it is impossible to get rid of intermediary knots. It occurs because those intermediary knots which are systemically necessary for functioning in the real world are systemically needed also in the world of a blockchain. Thus, we recreate the hierarchically ordered system of social institutes. However, we add obligation and transparency of implementation of contracts. It can't be made in the real world because of "human, too human." That is the slogans of reductionists were insolvent: it is impossible to get rid of system complexity of the world, and to here reduce an influence of a human factor it is quite real [10].

Already there is a concrete realization of the idea of a sharding, for example, Plasma [11] - it is the sharding-platform from Ethereum, that is, in the root of a hierarchy of blockchains, in this case, there will be Ethereum.

4.2. The answer to a challenge of a way of the establishment of consensus

The response to the second "deep" challenge of the need for designing of a way establishment of an agreement, can become Proof-of-Stake.

This option significantly less energy-intensive, than Proof-of-Work both much faster and scalable. On the one hand, it is less subject to the threat of "creeping" centralization of large pools of miners. But, on the other hand, avoiding one risk, this type of establishment of consensus introduces new problems.

Operation of validators on the different ends of a chain can lead to the crash system. That`s one threat of centralization replaced with another and what of them the lesser evil isn't apparent yet. However, the difference consists that Proof-of-Stake have a chance to be modified so that to avoid this threat, and at Proof-of-Work isn't present. The task includes in picking up parameters of realization Proof-of-Stake so that to keep advantages and to prevent risks. In practice, it isn't so easy to make it.

Therefore the actual realization of Proof-of-Stake is forced by something to renounce: the majority of the available options which aren't Proof-of-work (that is, Proof-of-Stake and others), are anyway partially centralized. In a blockchain community it is perceived unambiguously as the negative moment, therefore, a blockchain - software developers of an opportunity veil it. However, as protocols are open, blockchain enthusiasts, all the same, get to the bottom of an essence. For example, it has shown that the consensus of the Ripple network is a little bit centralized [12] also, as well as verification of transactions in the IOTA [13] system.

V. Conclusion

We have shown in this article that requires the blockchain industry in scalability and safety, comes down in many aspects to need of establishment of consensus [3]. And it can achieve employing the application of game-theoretic models. Thereby, it is possible to say that the game theory is a thematic priority for the development of the technology of a blockchain as the openly distributed ledger. It`s shown that the need for obtaining new results for games with imperfect information "covers" the most of the profound challenges facing blockchain technology. For justification of this provision to analyze various challenges are also allocated main of them. For each of the crucial challenges, it considered in what measure the answer to it is connected with the need of creation of new scientific results for some sections of game theory.

References

[1] Catalina C. (MIT), Gans J. S. (University of Toronto) Some Simple Economics of the Blockchain. [29.04.2018]. : http://www.cauchyinvestments.com/wp-content/uploads/2018/01/Some-Simple-Economics-of-the-Blockchain.pdf

[2] The future of cryptocurrencies: Bitcoin and beyond. [29.04.2018]: https://www.nature.com/news/the-future-of-cryptocurrencies-bitcoin-and-beyond-1.18447

[3] Genkin A., Mikheyev A. Blokcheyn: As it also works that waits for us tomorrow. – M.: Alpina Publisher, 2018. – 282 pages.

[4] Jesse Yli-Huumo, Deokyoon Ko, Sujin Choi, Sooyong Park, Kari Smolander. Where Is Current Research on Blockchain Technology?—A Systematic Review. [29.02.2018]: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477

[5] The "Digital Economy of the Russian Federation" program is approved by order of the Government of the Russian Federation of July 28, 2017. No 1632. [29.02.2018]: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.

[6] Bigi G., Bracciali A., Meacci G., Tuosto E. Validation of Decentralised Smart Contracts through Game Theory and Formal Method. [29.02.2018]: http://storre.stir.ac.uk/bitstream/1893/23914/1/bHalo_Degano2015.pdf

[7] Rusyaeva E.Yu., Saltykov S.A. Conceptual bases of the theory of active systems, their development in the theory of management of organizational systems: tendencies and prospects//Problems of Control. 2017. No. 4. Page 74-83.

[8] Yoad Lewenberg, Yoram Bachrach, Yonatan Sompolinsky, Aviv Zohar, Jeffrey S. Rosensche. Bitcoin Mining Pools: A Cooperative Game Theoretic Analysis. [29.02.2018]: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.9873&rep=rep1&type=pdf

[9] Lin Chen, Lei Xu, Nolan Shah, Zhimin Gao, Yang Lu, and Weidong Shi. Decentralized Execution of Smart Contracts: Agent Model Perspective and Its Implications. [29.02.2018]: http://fc17.ifca.ai/wtsc/Decentralized%20Execution%20of%20Smart%20Contracts%20-%20Agent%20Model%20Perspective%20and%20Its%20Implications.pdf

[10] Pryanikov M.M., Chugunov A.V. Blockchain as communication basis for the formation of the digital economy: advantages and problems. Kiberleninka. [29.02.2018]: https://cyberleninka.ru/article/n/blokcheyn-kak-kommunikatsionnaya-osnova-formirovaniya-tsifrovoy-ekonomiki-preimuschestva-i-problemy.

[11] Salvation From Cryptokitties Draws Near: Plasma AntiCataclysm. Open source PROOF-OF-ASSET protocol to facilitate [25.12.2017]: https://blog.bankex.org/salvation-from-cryptokitties-draws-near-plasma-anticataclysm-679adb2c1738.

[12] Peter Todd. Ripple Protocol Consensus Algorithm Review. May 11th 2015 [25.03.2018]: https://raw.githubusercontent.com/petertodd/ripple-consensu....pdf

[13] Eric Wall. IOTA is centralized. Jun 14, 2017. [27.03.2018]: https://medium.com/@ercwl/iota-is-centralized-6289246e7b4d.