Малыженков Павел Валерьевич

канд. экон. наук, доцент

ФГАОУ ВПО «Национальный исследовательский

университет «Высшая школа экономики»

г. Нижний Новгород, Нижегородская область

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИНДУСТРИИ 4.0: БЛОКЧЕЙН В СТРАХОВОМ СЕКТОРЕ

Аннотация: *рост числа онлайн-платежей и транзакций на финансовых рынках обостряет проблемы безопасности персональных данных и идентификации личности, что увеличивает спрос на технологии шифрования данных. Требуя более безопасных и качественных финансовых услуг, не все пользователи готовы оплачивать высокие транзакционные издержки. Технология распределенных реестров позволяет не только снизить затраты, но и повысить надежность транзакций любого типа. В перспективе такая технология может полностью трансформировать финансовый сектор и существенно снизить роль посредников.*

Ключевые слова: *использование технологий, блокчейн, страховой сектор, страхование.*

Malyzhenkov Pavel Valerievich

Cand. Sci (Economy), Associate Professor

National Research University

Higher School of Economics

Nizhni Novgorod, Nizhny Novgorod region

THE USAGE OF ENABLING TECHNOLOGIES OF INDUSTRY 4.0: BLOCKCHAIN IN THE INSURANCE SECTOR

Abstract: *the growth in the number of online payments and transactions in financial markets is exacerbating problems of personal data safety and identity security, which increases the demand for data encryption technologies. While demanding safer and better financial services, not all users are willing to pay high transaction costs. Distributed ledger technology can reduce costs and also increase the reliability of any*

1

type of transaction. In the future, such technology can completely transform the financial sector and significantly reduce the role of intermediaries

Keywords*: use of technology, blockchain, insurance sector, insurance.*

1. Distributed ledger technologies.

Distributed ledger technologies have revolutionized the world by transforming existing systems into more reliable, secure and scalable ones. Decentralized systems provide a trusted ledger among a group of nodes in a network that does not fully trust each other. Distributed ledgers have found their application in various sectors, including business, finance, Internet of things, industrial sector, etc.

The most successful examples of the integration of distributed ledger technology, and in particular its type of blockchain, appear in the financial sector. Blockchain is of significant interest for many areas, including insurance. This technology can help many users (entities) in the insurance industry cope with competitive challenges, develop online sales, improve the exchange of information between participants in the insurance market, and combat fraud.

2. How blockchain works.

Distributed ledger technology is an electronic database system distributed across multiple devices or network nodes. A key feature of DLT is the absence of a single regulatory authority. Distributed ledger technology allows information to be recorded and stored on a network that is both decentralized and distributed. These types of networks can be either public or private.

Networks based on a distributed registry system do not have a single control center. Instead, information is stored on several nodes of a peer-to-peer network at once, and an automatic consensus algorithm is used to update the data.

Data is transmitted across nodes (computers in the DLT network) that form the network, duplicated on them and synchronized. This way, each node independently updates itself to a complete copy of the registry. All nodes then vote to update the ledger and reach consensus on one of its copies. Each such update is protected by a

unique cryptographic signature. All this determines the security of the database and at the same time its transparency.

A distributed ledger is a database of specific assets. The latter can be of any nature, for example, electronic, financial, physical, all network participants have access to it from anywhere in the world through an identical, own copy of the registry. Any change in the registry is immediately reflected in all copies of the registries. The security and reliability of information is ensured by cryptographic protection methods, namely keys and electronic digital signature.

Blockchain is a platform for «smart contracts» which are small programs that can trigger specific actions when predefined conditions are met. In other words, a smart contact is an electronic algorithm that automates the process of concluding, registering, and executing contracts.

A smart contract has three key characteristics:

– observability of execution – the ability of subjects (to monitor the execution of each other's smart contract;

– verifiability – the ability of a party to a contractual agreement to prove to the arbitrator that the contract was fulfilled or violated;

– secrecy – knowledge and control over the content and execution of the contract should be distributed between the parties only to the extent necessary for the execution of this contract.

The smart contract code is executed automatically when a transaction is received.

3. Opportunities of blockchain technology in the insurance market.

As noted in the previous paragraph, distributed ledger technology is being studied and tested by insurance market actors. The insurance industry has a unique potential to use this technology in a system to increase efficiency and reduce costs by automating key processes. The insurance market needs a system based on digitized data and consisting of many participants who have limited trust in each other and work with the same data.

One of the key areas for the implementation of blockchain technology in insurance is a fundamentally new scheme for interaction between policyholders and insurers, which can contribute to a significant breakthrough in the insurance market; there

may be qualitatively new principles of interaction with clients that will allow the development of new insurance products, selling them via the Internet.

Note that blockchain technology can be useful for various types of insurance:

– medical insurance (reliable medical history for insurance payments);

– property insurance against accidents;

– insurance against natural disasters (insurance payments to participants in the agriculture and agro-industrial complex);

– car insurance, etc.

In addition, the process of insurance payments is simplified, since all actions are performed in real time with instant data updating, which simplifies and speeds up the payment process for both parties with high-quality verification of requests. In addition to the above, blockchain also simplifies administrative processes, such as document flow, thereby facilitating the verification of documents by insurance agents and optimizing the provision of insurance services to clients.

4. Limitations in the use of blockchain.

1. Scalability. Thanks to consensus-based validation mechanisms and continuous replication, and due to the ever-increasing amount of data stored and added, the scalability of the blockchain is still finite.

2. Decentralization. Even if blocks with less information are added to the chain, collecting data in real time and storing large volumes of information about insurance transactions ultimately forces us to reconsider the main principle of the blockchain – decentralization, since storing and processing it will require even more computing power every day. Thus, there is a contradiction with the main idea of a blockchain managed in a decentralized manner.

3. Security. According to the blockchain developers, cyber fraudsters can attack an insurance network operating on the blockchain, slow down time within the network, which in turn will complicate the transfer of data, messages between users, updating information and its final recording by transaction participants.

Besides, among the serious threats from hackers is the theft of personal data of policyholders, their addresses, information about concluded transactions, etc.

However, the distributed nature of blockchain databases makes hacking almost impossible for hackers, since to do this they need to simultaneously gain access to copies of the database on all computers on the network. The technology also makes it possible to secure the personal data of policyholders, since the hashing process is irreversible. Even if the original document or transaction is subsequently modified, it will end up with a different digital signature, signaling a discrepancy in the system.

References

1. Baliga, A., Subhod, I., Kamat, P., & Chatterjee, S. (2019). Performance Evaluation of the Quorum Blockchain Platform. Open access paper, 8.

2. Buchman, E., Kwon, J., & Milosevic, Z. (2019). The latest gossip on BFT consensus. Open access paper, 14.

3. Damgard, I. Nielsen, J.B., & Orlandi, C. (2018).Secure distributed systems. Electronic book, 332.

4. Cachin, C. (2017). Blockchain, cryptography, and consensus. Switzerland, Geneva, 38.