Blockchains in Spatial Data Security

Shaytura Sergey Vladimirovich
Russian University of Transport (MIIT)
Moscow, Russian Federation
swshaytura@gmail.com

Feoktistova Valentina Michaylovna
Russian State University of Tourism and Service
Moscow, Russian Federation
vfeoktistova@gmail.com

Minitaeva Alina Mazhitovna
Bauman Moscow State Technical University
Moscow, Russian Federation
aminitaeva@mail.ru

Ordov Konstantin Vasilievich
Plekhanov Russian University of Economics
Moscow, Russian Federation
post@ic-center.ru

***Abstract*— Blockchain is a technology that allows you to store information in distributed databases. This technology allows you to view the transaction history of all participants in the system. Usually blockchain technology is associated with cryptocurrencies, but such unique qualities of blockchain as transparency, decentralization, anonymity, equality and security allow to apply this technology in other areas as well. The article studies the principles of using blockchain technology in various spatial tasks as logistics systems, cadastral activities, tracking the movement of people, goods and things via the Internet based on global positioning. In logistics tasks, producing goods, they form a security token that follows the thing until the moment of delivery. In cadastral activity, a token, which takes into account the characteristics of the plot and its owners, connects with every plot of land. In public transport, all movements can be controlled and paid for using blockchains. Blockchain technology completely excludes the loss of things and people.**

Keywords*— *blockchain, spatial technologies, cryptographic methods, geoinformation technologies, geospatial innovation information, Bitcoin, cryptocurrency

I. INTRODUCTION

Blockchain technology is based on three principles: distribution, openness, security [1]. All users of the blockchain form a network in which each user stores a full copy of the data. All users in the network are equal, and in case of failure of the computer of several users, data will not be lost. The data in the blockchain is open to everyone. Each user can track data changes at any time. Only the owners of the data can change the data, and a private key can confirm the changes. They use cryptographic methods for informational security in the blockchain. The article analyzes the possibilities of using this technology in various spatial problems.

II. MATERIALS AND METHODS

There are many ways of user data security [2, 3, 4, 5]. They highlight follows:

- data copy technology, secure networking that provides the necessary trust in the software [6, 7, 8, 9];
- software verification technologies [10, 11, 12];
- methods of taking into account the human factor in the creation and operation of information systems [13, 14, 15, 16];
- cryptographic methods of data protection[17, 18, 19, 20, 21].

Blocked chains (blockchain) are open to all participants, so the ledger is available to all members. There are no centralized administrators, as it is a peer-to-peer network. All members verify and approve each transaction entered into the blockchain by consensus. However, there are validators that can view transactions and validate them. The two key characteristics of blockchain are trust and invariability. As in a business where transactions are based on trust, so members work on trust. Invariability is the possibility to prevent a transaction record, modification or deleting. When a member commits a transaction, it has a date and time stamp and is accompanied by a computer-generated key using the members ' private key.

Each subsequent transaction is similarly labeled and a new key is created that includes the earlier key. Thus, any hacking attempt will require unraveling the transaction password with a key, which is an impossible task. Even if it happened, the hacked register would be different from other copies and after the consensus; a consensus copy would delete and replace the process. What would happen if the change were genuine? There is a possibility of "branching" and temporary creation of two networks from one. A fork can occur in two ways; if two validators find a new block at almost the same time or if there are changes to the block validation rules. A soft fork occurs if the new rules are backwards compatible. A hard fork occurs if new software is introduced that is incompatible with earlier software.

They should understand that the ledger is, in fact, a transaction database. A blockchain makes sense if the ledger is common and many people, who may not know each other and do not necessarily trust each other, can make the transaction record. The solution in such a situation is to route such

transactions through a trusted intermediary known to everyone, but this increases the cost and processing time.

In Blockchain, a peer-to-peer network, in which authorization and validity of transactions is achieved through a process of negotiation between members, replaces such an intermediary. The ideal option for Blockchain is a multi-rank network that works without intermediaries, where the members of the network do not know each other enough to trust, and never the less the network requires openness and does not depend on capacity. However, if there is a need for centralized management, privacy, fast capacity and high scalability, then a normal distributed database seems to have a sense.

There are two types of the Blockchain, which are Public one and Private one. The most notable implementation of the Public Blockchain is the Bitcoin network. Here, the possible member to whom the system assigns the private key must open the wallet. Now a member can interact with others on the network, paying with bitcoins for goods, services, data, documents, etc.in the distant future, banks will go the way of Blockchain.

Another use of Blockchain is to track trading transactions, where the Blockchain is used to record transactions, acting as a notary and a personal data storage.

Public Blockchain has two drawbacks. The first is the verification process, which can take a long time as there are many users. The second is the block size, which can't be too large, so only the transaction data can be transfered, not the transaction object, such as documents. On the other hand, institutions such as government departments, industries, and companies can create and manage a private blockchains. Private Blockchain avoids these problems by limiting the number of users. Membership in the Private Blockchain is by invitation. Although others can see transactions they can't participate in. Administrators can easily change the rules governing private Blockchain and they could allow transaction rollback. Institutions appoint validators who are trusted by the institutions. Transaction costs are lower than in Public Blockchains and faulty nodes can be quickly detected and repaired.

Blockchain is the name of a distributed database, which is a sequential chain of blocks built according to certain rules that contain any information. Each block contains a timestamp and a link to the previous block. The blocks are linked chronologically and cryptographically. Cryptographic linking involves supporting rules for including new blocks in the chain and tracking attempts to modify existing blocks.

This approach is also called a distributed registry, referring to the fact that there is no centralized body (structure, regulator) that could dispose of such a chain of blocks at its own discretion. Accordingly, blockchain as a database has no centralized control. This database is open to any member of the network and the members ' own computers store it. The complete history of data changes is stored in the system and protected from changes by cryptographic mechanisms. Returning to the registry model, it seems to be as an electronically signed registry that is stored in a large number of copies in different locations.

Naturally, this storage model generates its own problems, which they often prefer not to mention. First, a complete copy of all data, including the history of all changes, creates a large demand for memory resources. They are required to store all these copies on the nodes involved in data processing. Keeping a history of changes means that resource requirements will increase rapidly as the system develops. Further, the spread of changes across all nodes significantly increases both the time of the transaction and its cost (in the sense of computation). It is also natural that there may be activities for which the open storage of information in a distributed network may be unacceptable (e.g., activities related to trade secrets or the storage of personal information).

One of the most well-known models of application of this technology is cryptocurrencies. In this case, the data blocks contain transactions describing the transfers of certain code sequences (digital coins) from one owner to another (Fig. 1).

Cryptocurrencies attract much attention, the word “bitcoin” has become almost nominal. At the same time, we should note that the word “currency” (digital or not) will almost always be naturally associated with state regulation. It is not clear how many such “currencies” the state will allow to have, etc. In other words, this undoubtedly important and interesting project (cryptocurrencies) obscures a bit other uses of the distributed register, which (it is important from a practical point of view) do not require state regulation at all. And we should note here that it should be typical for projects using databases. Distributed databases are another way to use blockchains.

Please do not revise any of the current designations. Hasq is a technology and a service based on it for maintaining distributed databases, implemented in the form of a decentralized system of servers [22].

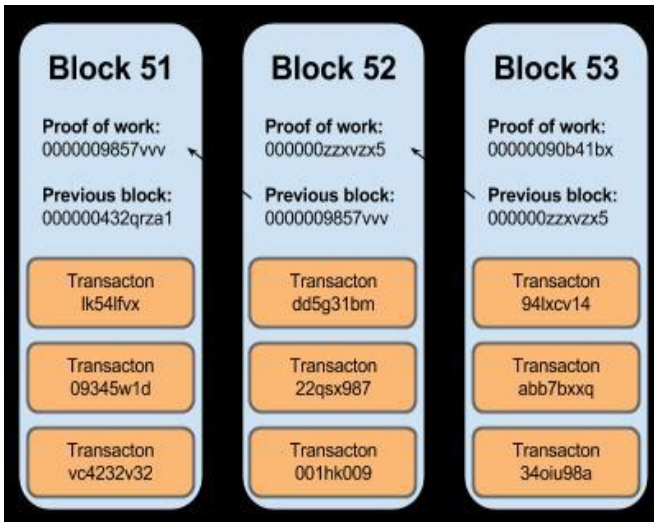

Fig. 1. The concept of transactions in the bitcoin chain

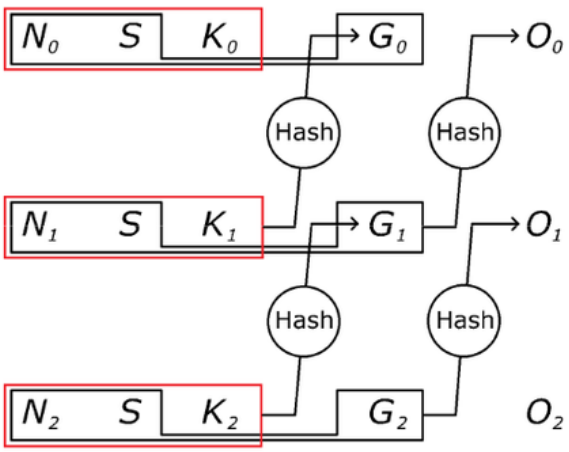

Fig 2.Hash chain of Hasq.

A database consists of a list of records that link together in a special way, using a hash function. Each entry has the following text fields separated by spaces: N, S, K, G, O, D, where N is an index number of a certain S. S (token) is the result of computing the hash function (hash) from digital data of random character, S represents a string of hexadecimal digits. Key (K), Generator (G) and Owner (O) are hashes, which they use for linking records. The number of G fields can be random but fixed within one database. D is optional data text field. Hash function links all fields. These links are presented on Fig. 2.

III. GIS-Services Based on Blockchains in the Logistics System

Information logistics system is a complex integrated system that organizes accounting, control, planning, purchase, supply and distribution of material and equipment. The main purpose of the information logistics system is to plan resource requirements and control their availability in warehouses. This system should monitor the availability of resources and warn about control standards excess. Information logistics system should also inform the decision-maker about possible suppliers of resources and find the best solution for the supply and sale. Information flows of the logistics system in the process of their movement pass through different levels of the organization structure and they are transformed at these levels [23, 24]. Primary information flows transform into material and information flows, material and information products and resources. It means that the process of information logistics creates additional material and information resources. The overall objective of information logistics at the enterprise is to ensure the competitiveness of the enterprise and its sustainable development.

Particular tasks of information logistics include:

- ensuring optimal use of limited material and information resources;
- ensuring optimal functioning of internal and external information flows;
- improving the efficiency of the enterprise management system, ensuring internal stability and high quality of meeting market needs;
- contributing to the creation of optimal stocks of material and information resources;
- ensuring high flexibility of the enterprise;
- reducing the duration of logistics cycles.

The information logistics system should control the flow of of material and equipment to the warehouse, that is, the system should rapidly monitor supplies and sales with the information flows. Management methods in logistics systems significantly differ with wide control of not only flows and stationary objects, but also mobile objects [25]. Accounting the spatial data relationship is very important for information and logic systems, as the expense and replenishment of resources is carried out in real space and time, which leads to the need to take into account the real spatial and logical relationships that exist in the process of transportation and delivery.

The life cycle [26] of the logistic delivery of goods passes the stages of production, configuration, shipment, acceptance and sale. When stages change, they conduct transactions in banking operations. In this case, for conducting these transactions it is expedient to use blockchains. Producing goods, they generate a token and transfer it to the next owner of the goods, and enter the produced action into the database. The system structure includes clients, GIS service, a distributed database and a blockchain.

IV. Using of Blockchains in Cadastral Activities

In the case of working out cadastral plans, there is no trust between the participators and there is a need for openness. The weakest link is the cadastral office, where data can be lost or they can conduct false transactions that cannot be detected immediately [27].

Let's examine the registration procedure of cadastral records which is based on blockchain. Various interested parties communicate with each other on request. The blockchain digitizes and places all information about the property (current owner, cadastral map). There is a contract that ensures that certain rules regulate the digitized space. They use the application as an interface to facilitate all transactions. The purchase and sale contract is processed into a hash code and placed in the blockchain. Banks, real estate agents, land buyers can confirm the authenticity of this purchase agreement and other documents through their unique digital signature (hash of the blockchain).

The algorithm for using the blockchain is following. First, the public key interface informs all interested parties. Second, they create a protocol that links as buyer to seller, as real estate, payment, bank, smart contract and registry. Third, they use specially improved smartphones that can process digital signatures, personal computers and other gadgets to interact

with the phone through some form of authentication. All this can work within the framework of the blockchain.

In Moscow, they intend to extensively use blockchain technology in the city management, in particular, in the spheres of housing and communal services, health care, cadastral registration, subsidying and state purchase contracts [27].

V. Blockchain and Internet of Things

Another important area where they can effectively use blockchain together with geospatial technologies is the Internet of things [28, 29, 30]. Today, the Internet of things creates an image to be a complex network of people and objects that transmit data to each other [31, 32]. Some questions about it appear. What kind of data are there? How are they verified, how are things and people protected from illegal access and processes? For example, can a car with an anti-theft alarm system be stolen? So far, there is not any anti-theft alarm system, which guarantees it. The use of blockchain technology can solve this problem. If the chain contains the anti-theft data, tone person cannot change them, since all transactions in the blockchain are stored in all previous and subsequent data. Blockchain and smart contracts can be the basis of a managed, transactional Internet, where machines observe rules and follow algorithms, provide the kinds of verification usually associated with a third party. Business process management can engage in the internal process of each object and act as web on one side of the transaction or the other. Smart contracts extend the ability to manage business processes outside the walls of the organization and can become intermediaries between two business partners.

VI. Blockchain and Geospatial Data

Imagine a traveler in a public transport system who uses a smart mobile with tokens. When a person takes a bus, the crypto-spatial layer marks the getting on and getting off point and automatically charges from the traveler's spatial wallet and credits to the transport company's spatial wallet. There is no need to use cards or recharge cards. Debits and credits are counted instantly and the transaction automatically accords with the blockchain [25, 29, 33, 34, 35].

They can monitor movements and transfer of goods and automatically calculate and debit the cost of shipping. Data can include satellite data, maps, land plot data, 3D visualization data, etc. In this way, they can easily estimate and distribute spatial data of satellites, drones, and even terrain measurements. They can integrate data security through tokens.

VII. Discussion of Results

Human activity continuously connects with the flow of data, documents and money. It is very difficult to control this process. Employees of banks, shops very often tend to abuse their official status.

Blockchain is a technology of reliable distributed data storage and the data can be of any types of human activity products [36, 37, 38].

A blockchain is a chain of data blocks where each block links to the previous one. New blocks always add strictly to the end of the chain [40, 41, 42].

All users form a distributed database, each computer stores a complete copy of all blocks. It is impossible to destroy the data in such a database, because you have to destroy all the computers located in different places. Each user strengthens this network. In a distributed network database, there are no moderators, supervisors, managers, organizers, as all users are equal. They can use the cryptography, which increases the data security, to transfer data.

VIII. Conclusion

The use of blockchain technology allows fully controlling the spatial movement of produced goods, and in combination with spatial positioning technology eliminates possible thefts. Blockchain will help to reduce the cost of controlling the distribution of products, increase the level of trust between the participants of the exchange in logistics transportations.

References

[1] E.A. Khrisanova, “Development of methods for protecting a distributed geoinformation database” [“Razrabotka metodiki zashchity raspredelennoi geoinformatsionnoi bazy dannykh”], Slavic forum [Slavyanskii forum], no. 3 (17), pp. 163 – 167, 2017.

[2] Probabilistic Modeling in System Engineering / By ed. A. Kostogryzov – London: IntechOpen, 2018. 278 p. DOI: 10.5772/intechopen.71396.

[3] Markov A.S., Fadin A.A., Tsirlov V.L. Multilevel Metamodel for Heuristic Search of Vulnerabilities in the Software Source Code, International Journal of Control Theory and Applications, 2016, vol. 9, No 30, pp. 313-320.

[4] Zegzhda, P., Zegzhda, D., Pavlenko, E., Dremov, A. Detecting Android application malicious behaviors based on the analysis of control flows and data flows (2017) ACM International Conference Proceeding Series, pp. 280-286. DOI: 10.1145/3136825.3140583

[5] Zegzhda, D.P., Usov, E.S., Nikol’skii, A.V., Pavlenko, E.Y. Ensuring Secure Data Input/Output Operations for SGX ENCLAVE (2018) Automatic Control and Computer Sciences, 52 (8), pp. 1036-1041. DOI: 10.3103/S0146411618080321

[6] D. Maevsky, V. Kharchenko, M. Kolisnyk, and E. Maevskaya, “Software reliability models and assessment techniques review: Classification issues”, 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), IEEE, pp. 894–899, 2017. DOI: 10.1109/IDAACS.2017.8095216

[7] E.G.Vorobiev, S.A. Petrenko, I.V. Kovaleva, and I.K. Abrosimov, “Organization of the entrusted calculations in crucial objects of informatization under uncertainty”, Proceedings of 2017 20th IEEE International Conference on Soft Computing and Measurements, SCM, no. 20, pp. 299 – 300, 2017. DOI: 10.1109/SCM.2017.7970566.

[8] Markov A., Barabanov A., Tsirlov V. Models for Testing Modifiable Systems. In Book: Probabilistic Modeling in System Engineering, by ed. A.Kostogryzov. IntechOpen, 2018, Chapter 7, pp. 147-168. DOI: 10.5772/intechopen.75126.

[9] Markov A., Barabanov A., Tsirlov V. Periodic Monitoring and Recovery of Resources in Information Systems. In Book: Probabilistic Modeling in System Engineering, by ed. A.Kostogryzov. IntechOpen, 2018, Chapter 10, pp. 213-231. DOI: 10.5772/intechopen.75232.

[10] Petrenko, A.S., Petrenko, S.A., Makoveichuk, K.A., Chetyrbok, P.V.: Protection Model of PCS of Subway from Attacks Type «Wanna cry», «Petya» and «Bad rabbit» IoT. In: Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic

Engineering (ElConRus 2018). IEEE, pp. 945 – 949 (2018). DOI: 10.1109/EIConRus.2018.8317245.

[11] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, "Panning for gold: Automatically analysing online social engineering attack surfaces", Computers & Security, vol. 69, pp. 18–34, 2017.

[12] V.N. Ivanova, A.L. Poltarykhin, A. Szromnik, and O. Anichkina, "Economic policy for country's digitalization: a case study", Entrepreneurship and Sustainability Issues, no. 7(1), pp. 649-661, 2019.

[13] B.I. Skorodumov, O.B. Skorodumova, and L.F. Matronina "Research of Human Factors in Information Security", Modern Applied Science, vol. 9, no. 5, pp. 287–294. 2015.

[14] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks" Journal of Information Security and Applications, vol. 22, pp. 113–122, 2015.

[15] F. Mouton, L. Leenen, and H.S. Venter, "Social engineering attack examples, templates and scenarios", Computers & Security,] vol. 59, pp. 186–209, 2016.

[16] Nader Sohrabi Safa, Rossouw von Solms, and Lynn Futcher, "Human aspects of information security in organisations", Computer Fraud & Security, no. 2, pp. 15–18, 2016.

[17] S.V. Belim, and N.F. Bogachenko, "Distribution of Cryptographic Keys in Systems with a Hierarchy of Objects", Automatic Control and Computer Sciences, vol. 50, no. 8, pp. 777–786, 2016.

[18] A. Barabanov, and A. Markov, "Modern Trends in The Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria", Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 30-33. DOI: 10.1145/2799979.2799980.

[19] A. Markov, D. Luchin, Y. Rautkin, and V. Tsirlov, "Evolution of a Radio Telecommunication Hardware-Software Certification Paradigm in Accordance with Information Security Requirements", Proceedings of the 11th International Siberian Conference on Control and Communications (Omsk, Russia, May 21-23, 2015). SIBCON-2015. IEEE, 1-4. DOI: 10.1109/SIBCON.2015.7147139.

[20] V. Yemelyanov, N. Yemelyanova and A. Nedelkin, "Neural network for decision support to determine the operating mode of lined equipment", Paper presented at the MATEC Web of Conferences, p.224, 2018. doi:10.1051/matecconf/201822404005

[21] A. Boiko, V. Shendryk, and O. Boiko, "Information systems for supply chain management: uncertainties, risks and cyber security", Procedia Computer Science, vol. 149, pp. 65 – 70, 2019. DOI: 10.1016/j.procs.2019.01.108.

[22] G. G. Trubach, "Environment development for monitoring commodity and transport flows based on blockchain technologies" ["Razrabotka sredy monitoringa tovarno-transportnykh potokov na osnove tekhnologii blokchein"], Collection of works of the 74th scientific conference of students and postgraduates of the Belarusian state University: in 3 parts [Sbornik rabot 74-i nauchnoi konferentsii studentov i aspirantov Beloruskogo gosudarstvennogo universiteta: v 3 chastyakh], pp. 96-99, 2017.

[23] V. Tatarinov, and A. Kirsanov, "Enhancement of monitoring systems for the transport of dangerous goods by road", 2019 IOP Conf. Ser.: Mater. Sci. Eng. 492 012017

[24] V.YA. Tsvetkov, "Logistics information distributed systems" ["Logistika informatsionnykh raspredelennykh sistem"], Prospects of science and education [Perspektivy nauki i obrazovaniya], no. (4)22, pp. 18 -22, 2016.

[25] S.V. Shaitura, Yu.P. Kozhaev, K.V. Ordov, T.A. Vintova, A.M. Minitaeva, and V.M. Feoktistova, "Geoinformation services in a spatial economy", International Journal of Civil Engineering and Technology, vol. 9, no. 22, pp. 829-841, 2018.

[26] V.V. Dik, and S.V. Shaitura, "Life cycle of information systems" [ZHiznennyi tsikl informatsionnykh sistem], Vestnik MGTU MIREA, no. 3 (4), pp. 116 – 129, 2014.

[27] S.A. Pavlov, "Perfection of technology of formation of territorial zones of objects of technogenic safety at introduction of the state ground cadastre" [Sovershenstvovanie tekhnologii formirovaniya territorialnykh zon obieektov tekhnogennoi bezopasnosti pri vvedenii gosudarstvennogo zemelnogo kadastra] Slavic forum [Slavyanskii forum], no. 3 (17), pp. 144 – 149, 2017.

[28] S.V. Shaitura, Yu.P. Kozhaev, K.V. Ordov, A.V. Antonenkova, and N.A. Zhenova, "Performance evaluation of the electronic commerce systems", Espacios, vol. 38, no. 62, p.11, 2017.

[29] S.V. Shaitura, A.M. Minitaeva, K.V. Ordov, and V.V. Shaparenko, "Virtual enterprises in a spatial economy", International Journal of Recent Technology and Engineering (IJRTE), vol. 7, no. 6, pp. 719 – 724, 2019.

[30] S.V. Shaitura, K.V. Ordov, I.G. Lesnichaya, Yu.D. Romanova, and S.S. Khachaturova "Services and mechanisms of competitive intelligence on the internet", Espacios, vol. 39, no. 45, p. 24, 2018.

[31] J.Y. Astier, I.Y. Zhukov, O.N. Murashov, "Smart Building Management Systems and Internet of Things. IT Security", [S.l.], vol. 24, no. 3, pp. 18−29, july 2017. ISSN 2074-7136.

[32] Malte Burkert, Heiko Krumm, and Christoph Fiehe, "Technical management system for dependable Building Automation Systems", 2015 IEEE 20th Conference on Emerging Technologies & Factory Automation (ETFA), pp. 1 - 8, 2015. DOI: 10.1109/ETFA.2015.7301656

[33] Zhaohui Wu, Jianwei Yin, Shuiguang Deng, Jian Wu, Ying Li, and Liang Chen, "Modern Service Industry and Crossover Services: Development and Trends in China", IEEE Transactions on Services Computing, vol. 9, no. 5, pp. 664-671, 2016. DOI: 10.1109/TSC.2015.2418765

[34] Usman Raza, Parag Kulkarni, and Mahesh Sooriyabandara "Low Power Wide Area Networks: An Overview", IEEE Communications Surveys & Tutorials, vol. 19, no. 2, pp. 855-873, 2017. DOI: 10.1109/COMST.2017.2652320

[35] Keyi Zhang, and Alan Marchiori, "Crowdsourcing low-power wide-area IoT networks", 2017 IEEE International Conference on Pervasive Computing and Communications (PerCom), pp. 41-49, 2017. DOI: 10.1109/PERCOM.2017.7917849

[36] R. M. J. Rathnayaka, KTMU Hemapala, "Developing of scalable SCADA in view of acquiring multi-protocol smart grid devices", 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), pp. 182 – 187, 2016. DOI: 10.1109/AEEICB.2016.7538269

[37] Saveen A. Abeyratne, and Radmehr P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger", International Journal of Research in Engineering and Technology, no. 05 (09), pp. 1–10, 2016.

[38] A. B. Ayed, "A conceptual secure blockchain-based electronic voting system", International Journal of Network Security & Its Applications, vol. 9, no. 3, 2017.

[39] R.Hanifatunnisa, and B. Rahardjo, "Blockchain based e-voting recording system design (2018)", Proceeding of 2017 11th International Conference on Telecommunication Systems Services and Applications, TSSA 2017, pp. 1-6, January 2018.

[40] D. Kirilova, N. Maslov, T. Astakhova, "Prospects for the introduction of blockchain technology into a modern system of education", International Journal of Open Information Technologies, vol. 6, no. 8, 2018.

[41] F. Caldieraro, J. Z. Zhang, M. Jr. Cunha, and J. D. Shulman, "Strategic Information Transmission in Peer-to-Peer Lending Markets", Journal of Marketing, vol. 82, no. 2, pp. 42- 63, March 2018

[42] W. Liu and L-Q Xia, "An Evolutionary Behavior Forecasting Model for Online Lenders and Borrowers in Peer-to-Peer Lending." AsiaPacific Journal of Operational Research, vol. 34, no. 01, 2017.