Comparison of integrable Blockchain technologies in the processes of digitalization of sectors of the national economy

Oleg A. Malafeyev[1], *Ahad* O. Qodirov[2], *Irina* V. Zaitseva[3*], *Tatyana* M. Kosovskaya[2], *Svetlana* V. Belyaeva[4], *Marina* G. Leshcheva[5], and *Larisa* V. Kuleshova[5]

[1]Saint-Petersburg State University, Faculty of Applied Mathematics and Control Processes, Universitetskaya nab., 7/9, St. Petersburg, 199034, Russia
[2]Saint-Petersburg State University, Mathematics and Mechanics Faculty, Universitetskaya nab., 7/9, St. Petersburg, 199034, Russia
[3]Russian State Hydrometeorological University, Institute of Information Systems and Geotechnologies, Voronezhskaya Street, 79, St. Petersburg, 192007, Russia
[4]Branch "Plekhanov Russian University of Economics" in Pyatigorsk, Pyatigorsk, Kuchura Street, 8, 357500, Russia
[5]Stavropol State Agrarian University, Zootekhnicheskiy Lane, 12, Stavropol, 355035, Russia

Abstract. Today all over the world digital technologies are a priority for the development of the healthcare sector. Digitalization increases the availability of medical services and improves their quality without a significant increase in healthcare costs, while the development of digital medicine is impossible without the participation of public and private partnerships. Russia has not become an exception, where several world-wide information and analytical projects are already being implemented, one of which is Blockchain technologies. However, the question of which Blockchain technology to use is still open. In this article, the authors compare the economic and technical characteristics of the three most popular Blockchain technologies that are used in the digitalization of healthcare and give their recommendations on the digitalization of the social insurance healthcare system in the Russian Federation.

1 Introduction

Today, Blockchain technologies are actively used in international medical practice both at the state level and at the level of the private market. The international healthcare system itself can be conditionally divided into three groups: State (Canada, Great Britain, Denmark, Portugal, Ireland, Greece, Italy, Spain, etc.), private (USA, South Korea, Switzerland, etc.) and social insurance (Russian Federation, China, Japan, France, Germany, Estonia, etc.). The state system (another name is the Beveridge financing model) differs from other health care systems by providing free medical services and ensuring equal access to them for all citizens of the country. Most of the funding comes from public sources. The administrative structure

* Corresponding author: irina.zaitseva.stv@yandex.ru

of the country exercises full control over the medical infrastructure (regulation of legislative standards, the choice of a development strategy, the integration of innovative technologies, etc.). In this regard, the state is the main producer and supplier of all comprehensive medical services 1.

In a previous article, the author analysed the strengths and weaknesses of three Blockchain solutions that are used in the digitalization of world medical systems. The considered Blockchain solutions were Ethereum, Tencent Chain, and Hyperledger Fabric. This article will conduct a comparative analysis of the listed decentralized Blockchain solutions

A comparative analysis of Blockchain solutions was carried out by three graduate students of the Faculty of PM-PU of St. Petersburg State University under the guidance of Professor, Doctor of Physics and Mathematics, Oleg Malafeev. Although only one student developed the code for each of the platforms, the research team worked together to compare the data with the assistance of the professor mentioned above. First, the group built three selected blockchain networks. Further, smart contracts were created in them. We used six virtual machines (hereinafter referred to as VMs), each with a dual-core processor, 8 GB of RAM and 100 GB of storage, running a 64-bit Ubuntu 14.04 operating system on the Google Cloud Platform. The research team then tested the considered blockchain platforms by creating medical metrics in them, sending transactions, and executing smart contracts on them.

2 Method

Since medical data can be extremely large (the entire medical history of a patient can take up gigabytes of information - MRI images, ultrasound, video recordings of cardiac surgery, etc.), sending them via the Blockchain is inappropriate and extremely costly. In addition, the transfer of such volumes of information can take a huge time, which the patient may not have. In this regard, the scientific group used hybrid types of the Blockchain, which allow storing all information (in an anonymized, hashed form) in the cloud storage (or on the servers of medical institutions), and within the Blockchain only a hashed link to the storage is transmitted. The results of the experiment are shown in Table 1.

The calculation of consumption of average indicators of electricity consumption was based on the methodology of the Canadian consulting company MNP (total electricity consumption for the entire period, the total number of created blocks for the entire period, the total number of transactions for the entire period) 1,1. The results were measured within 1 month.

Table 1. Comparison results of Blockchain technologies.

Platform	Ethereum	Hyperledger Fabric	Tencent Chain
Smart contract type	Second generation	Second generation	Second generation
Programming language	Solidity, Serpent and LLL	Go and Node.js for Chaincode	JavaScript for smart filter
Network resolution	Allowed / Without permission	Allowed	Allowed
		Apache License v2.0	GPL v3.0

Open source license	Go-Ethereum: LGPL v3.0, CPP-Ethereum: GPL v3.0, Py-Ethereum: MIT License, Ethereum J: GPL v3.0, Parity: GPL v3.0		
Applications	MedRec, Patientory, Nebula Genomics, HealPoint, MedCredits, Healthureum, Zealeum, Robomed Network, Prescrypt, Aenco, Sunny Lake Patient monitoring, etc.	IBM blockchain Healthcare, Healthchain, Medicalchain, Clinical data sharing, Institutional Review Boards (IRB) regulation enforcement, mobile healthcare, medical data storage/access, etc.	Bambusoft, Block data SAS, CrimsonLogic, Enuke Software, Indra Sistemas, Minddeft Technologies, Mphasis Ltd, VTeam Financial Technology, etc.
Electricity consumption per 1000 transactions	Min - 0.9 kWh Max - 3.1 kWh	Min - 0.3 kWh Max- 0.7 kWh	Min - 0.5 kWh Max- 1.8 kWh
Average number of transactions per second	over 2,000	over 2,000	over 2,000
Average integration time into existing digital solutions	less than 5 working days	less than 10 working days	less than 5 working days

The calculation of consumption of average electricity consumption indicators was based on the methodology of the Canadian consulting company MNP (total electricity consumption for the entire period, the total number of blocks created for the entire period, the total number of transactions for the entire period, the total number of verified megabytes for the entire period, etc.). The results were measured within 1 month.

3 Discussion

Ethereum - the scientific group built a Blockchain network using Go-Ethereum. Then I sent transactions (medical data in 1 megabyte) and checked that the transaction input for both servers was the same. Finally, the group wrote, compiled, deployed, and executed smart contracts using Solidity on the blockchain network they created. The whole process of building the blockchain network took about 30 minutes, the speed of one transaction was 5 minutes (time estimates assume that the transaction was confirmed in the first block after the transaction was sent), the training time to work with the system for an undergraduate student (St. Petersburg State University) was about 5 days. The average power consumption was 2.75 kWh per 10,000 transactions.

Hyperledger fabric - the scientific group built a distributed network using Hyperledger Fabric technology. The group then sent transactions (health data stream, 1MB in size) to test connectivity to the network and initiated the execution of smart contracts using Chaincode in the Go language. The whole process of building the Blockchain network took about 45 minutes, the data transfer rate was 3 minutes, the total training period (medical data entry, maintenance and access requests) for undergraduate students was about 10 days. The average power consumption was 0.95 kWh per 1000 transactions. This indicator is 2.89 times lower than the Ethereum energy consumption indicator, which indicates the energy efficiency of the Blockchain system in question.

Tencent Chain - by building a network of distributed registries and sending transactions between nodes, the research team was convinced of the speed and operability of the network. After that, the group created information flows (medical records of patients) for the dissemination of key-value data pairs. Finally, the group examined the overall security of the network and its throughput. The whole process of building the Blockchain network took about 30 minutes, the data transfer rate was 5 minutes. The total period of learning how to work with the system for bachelors took 2 days, which indicates a simple use interface. The average power consumption was 1.25 kWh per 1000 transactions. This indicator is lower than Ethereum by 2.2 times, but still exceeds Hyperledger Fabric by 1.32 times.

Based on experimental data conducted by our research team at St. Petersburg State University, MultiChain is the simplest distributed network platform in terms of setup, use and speed. Setting up Ethereum as a permissioned network took longer than the MultiChain discussed above.

Hyperledger Fabric contains more layers of verification in its network (to improve security and manageability) than other examples. This results in longer integration times and also complicates the interaction between network participants compared to other platforms. But in terms of the level of data protection and the level of energy consumption, this is the most efficient Blockchain technology out of the three considered.

Installing the required software (in existing medical platforms) for Tencent Chain and Ethereum is also faster than installing software in Hyperledger Fabric. On the other hand, Ethereum and Hyperledger provide full-featured smart contract capabilities, while smart contract support for Tencent Chain is limited. Smart contracts are easy to read and easy to program.

As for biometric medical applications, the main characteristics of the three platforms are as follows. Ethereum is supported by a large number of developers around the world. The openness of the code makes it an excellent choice given the long-term sustainability of the platform on which medical applications are based. Hyperledger Fabric, due to the multi-layered access control system, makes this language universal in the field of data storage security and manageability. Tencent Chain, being a permissioned blockchain, is very easy to learn and use, making it the most efficient in terms of pervasive integration.

Based on the Federal laws on the protection of personal data and on the Government Decrees (described above) on healthcare, the author comes to the conclusion that the key provisions of the digitalization of medicine in the Russian Federation are the protection of personal data and the speed of information transfer. Also, do not forget the cost of technology, which directly depends on the level of energy consumption. In this regard, the author believes that the most suitable Blockchain technology for the digitalization of the social insurance healthcare system of the Russian Federation is the decentralized Hyperledger Fabric system (its hybrid form).

Having decided on Blockchain technology, the author proposes to compare it with technological solutions existing on the world and Russian markets (with medical database management systems), such as Oracle 4, Apache Cassandra 5 and Uniform State Health Information System (Unified State Health Information System) 6. A database management system (Distributed Database Management System, abbr. - DDBMS) is a cumulative association, consisting of several interconnected databases distributed over a network.

The first key advantage of the proposed Hyperledger Fabric Blockchain technology in the digitalization of medicine is decentralized control. DDBMS, although technically distributed (on levels - federal, regional, local; on server structures - medical clinics, outpatient centers, etc.; on medical areas of the server association - cardiology, therapeutic, etc.), nevertheless is managed centrally, while the Blockchain network is a peer-to-peer decentralized database management system (each individual node, subject to predetermined protocols, operates independently of the other) 7.

Thus, Blockchain technology is suitable for storing personal medical data precisely because it does not depend on a specific object in the network (for example, a hospital, a healthcare provider, a patient, etc.). Blockchain network participants are in partnership with each other, without transferring control to an intermediary, individual or central authority. Therefore, if one server is “hacked”, firstly, the stored medical information is not threatened by a leak (fragmented anonymized form), and secondly, the system will continue to maintain a functional basis.

The second key advantage of Hyperledger Fabric is the immutability of stored data on the network. DDBMS supports the functions of creating, reading, updating and deleting stored information, like all database systems, while Blockchain technology supports only the creation and reading functions (deletion can only be done with the help of an administrator, while the change is displayed in the change register) 8. Thus, the Blockchain is suitable as an immutable ledger for recording important information (for example, patient history, insurance claims records, prescribed medicines, and so on).

The third is the origin of the data. In DDBMS, ownership of stored digital assets (medical history, personal medical data, etc.) is indirectly owned by the administrator (who owns the server owns the information). In Blockchain, ownership belongs only to the patient. In addition, the ownership right itself can be changed by the owner of the digital asset in accordance with pre-defined cryptographic protocols. In addition, the origin of a digital record in the system under consideration is strictly traced, which increases the reliability of the data (at any time it is possible to check by whom and when this or that record was created, as well as who viewed it). Thus, distributed registries are suitable for managing critical digital medical assets of patients.

The fourth advantage is the high security of stored data and their complete confidentiality, which is achieved using cryptographic algorithms. For example, the Bitcoin blockchain technology uses a 256-bit secure hashing algorithm (SHA-256) and a cryptographic hash function as a cryptographic security system, while Hyperledger Fabric uses the PBFT (Practical Byzantine fault tolerance) consensus algorithm. In addition, Blockchain uses a 256-bit digital signature algorithm and an asymmetric cryptography algorithm to generate and verify high-security public and private keys, thereby ensuring the security of ownership of digital assets (records) of patients.

All of the above advantages of the Hyperledger Fabric Blockchain show that the technology in question is much more stable and secure in comparison with the digital healthcare technologies currently used in the Russian Federation.

But, in addition to the obvious advantages of Blockchain technology in the digitalization of the social insurance health care system of the Russian Federation, there are a number of problems that arise during the use of the technology in question. Below is a list of potential threats that may arise when using distributed registries in the digitalization of domestic medicine.

The first problem is related to the personal privacy of the network member. Since each participant "sees everything" in the Blockchain network, increased transparency is considered a weak point of the technology. Also, even if a user is "anonymized", that user can still be re-identified. This happens through the analysis of publicly available information about completed transactions in the blockchain network. Consequently, distributed registries provide only partial anonymity (with a certain approach, indirect methods, the user can be identified by another network member) 9.

This problem is critical for the storage of medical information, since patient data in the Russian Federation, according to the law, must always remain confidential. And incomplete confidentiality of personal information or the possibility of indirect verification of personality leads to the leakage of this information to third parties, which is administratively prohibited throughout the country. Therefore, the solution to this problem can be the use of a hybrid Hyperledger Fabric Blockchain, where the stored information is not transferred from node to node but is stored on secure servers in a hashed form. Passing a hash link solves the problem of indirect user identification (more on hash links below).

The second problem is related to the speed of data transfer and their scalability. The time of one transaction, in the classic Hyperledger Blockchain (and in any other Blockchain), can take a long time (depending on the protocol and on the volume of the transfer). Such rate limiting can limit the scalability of the network, and therefore slow it down even more. For example, the Proof-of-Work protocol, on average, can carry out about 288,000 transactions per day (or about 3.3 transactions per second). For comparison, we can draw a global payment system Visa, which, using credit cards, makes 150 million transactions per day (or about two thousand transactions per second). The theoretical maximum transaction speed for Bitcoin is seven transactions per second 10. This is due to the 1-megabyte block size limit (in the current protocol). The theoretical maximum number of transactions for Visa is 4000 transactions per second 11.

This shows that scalability and data transfer speed are a problem area of the technology under consideration, especially when it comes to transferring large amounts of information (MRI, CT images, results of complex analyze, etc.) 12. The use of the Hyperledger hybrid Blockchain, a three-stage security system, and the transfer of small hash links instead of large medical data solves the problem of data transfer speed and scalability (one hash link can take only tens of kilobytes of information).

His blockchain "hash link" methodology works in three steps. The first step is data encryption (for example, encryption of personal identifying information and medical history) 13. At the second stage, the data stored in the network is transferred outside of it (to the servers of organizations participating in the network - hospitals, clinics, etc.). At the third stage, when two participants interact, the transfer occurs only by encrypted links (with an access key) to the place where the required information is stored 14. In addition, there are several new blockchain solutions on the market now, such as BigchainDB 15, Ripple, Solana, Stellar, Universa, Waves (Russian hybrid Blockchain -solution), which provide a significantly higher transaction speed than the Bitcoin blockchain, which can also solve the problem of speed and scalability.

The latest threat to Hyperledger Fabric technology is the 51% attack threat. A blockchain network can suffer from a “51% attack,” which occurs when there are fewer “honest” nodes in the entire network than malicious ones (or when 51 percent collude). A schematic explanation of this threat is presented in Figure 1.

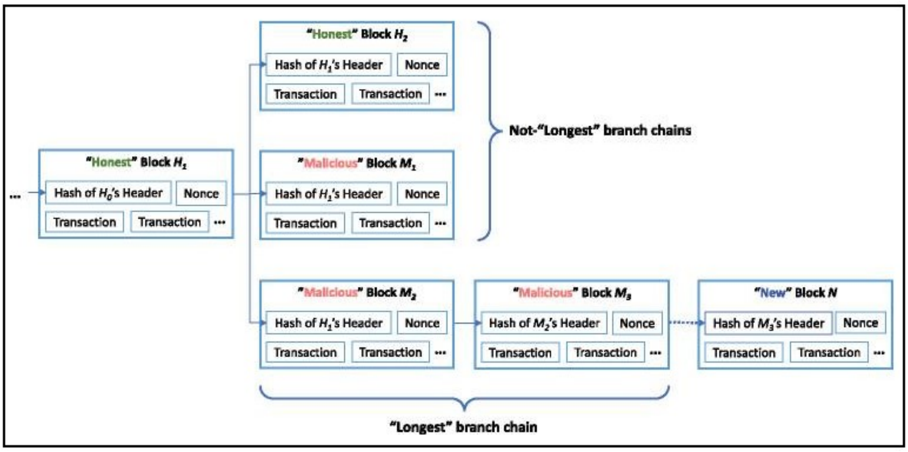

Fig. 1. Schematic representation of the Blockchain attack 51%.

4 Conclusion

The solution to this problem is the verification of all network users. When the Blockchain system is devoid of anonymous users, capturing operational capacity is technically impossible. In other words, when all participants in the decentralized Blockchain network (medical producers, insurance agents, regulatory authorities, patients, etc.) are identified and pre-identified, none of the participants will be endowed with computing power that would allow them to take over the entire system.

After conducting a comprehensive analysis of the technical capabilities and economic and social benefits of decentralized technologies, the author proposes a Blockchain model that will allow digitalization of the domestic social and insurance health care system using distributed registries. To date, the proposed technological solution is being developed by a scientific group, which includes the author.

References

1. A. Rieger, F.J. Guggenmos, Lockl, G. Fridgen, and N. Urbach, MIS Q Exec **18(4)**, 263-279 (2019)
2. J. Sedlmeir, U. Buhl, G. Fridgen, R. Keller, Business & Information Systems Engineering **62**, 599-608 (2020)
3. Measuring Bitcoin Energy Consumption and Efficiency (2020). https://bitcoinassociation.net/en/measuring-the-energy-consumption-and-efficiency-of-bitcoin/
4. Oracle. The Oracle Database (2021). https://www.oracle.com/database/index.html
5. The Apache Software Foundation. Apache Cassandra (2020). http://cassandra.apache.org/
6. Unified State Health Information System (2022). https://egisz.rosminzdrav.ru/
7. S. Meunier, Blockchain Technology—a Very Special Kind of Distributed Database. Medium (2020). https://medium.com/@sbmeunier/blockchain-technology-a-very-special-kind-of-distributed-database-e63d00781118
8. T. McConaghy, R. Marques, A. Müller, BigchainDB: A Scalable Blockchain Database (2021). https://www.bigchaindb.com/whitepaper/

9. A. Abbas, Understanding Privacy: How Anonymous can Bitcoin Payments be? (2020). bitcoinist.net. http://bitcoinist.com/understanding-privacy-anonymous-bitcoin/
10. Blockchain Luxembourg S.A. Confirmed Transactions Per Day (2019). https://blockchain.info/charts/n-transactions
11. Visa Inc. Visa Acceptance for Retailers (2019). https://usa.visa.com/run-your-business/small-business-tools/retail.html
12. C.B. Kalis, E. Mitchell, E. Pupo, A. Truscott, Blockchain: securing a new health interoperability experience. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST (2018)
13. R. Prakash, Adoption of blockchain to enable the scalability and adoption of accountable care. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST (2016)
14. R. Krawiec, D. Barr, J. Killmeyer, Blockchain: opportunities for health care. ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST (2019)
15. BigchainDB GmbH. BigchainDB The scalable blockchain database (2018). https://www.bigchaindb.com