Architecture of the Digital Distributed Platform for Medical Consiliums

Golosovskiy M.S.*, Bogomolov A.V., Tobin D.S.

St. Petersburg Federal Research Center Russian Academy of Sciences, St. Petersburg 199178, Russia
**Corresponding author. Email: gniiivm-g@ya.ru*

ABSTRACT
The developed architecture of a digital distributed platform for medical consultations is described in the form of a blockchain network that unites automated workstations of specialists, managed by the head of the council, and nodes with read-only permissions (audit nodes). The blockchain network provides an immutable record of all data in platform nodes throughout the network and acts as a central communication channel and information storage. The use of closed blockchain technologies ensures the confidentiality of the collected and processed information about the anamnesis and the current state of the patient, providing users with quick access to relevant protected information remotely, minimizing the possibility of third-party interference and information distortion.
Keywords: *Medical consiliums, closed blockchain, network expertise, digital medicine, distributed ledger technology, distributed information processing, replicated distributed database*

1. INTRODUCTION

To establish a diagnosis, determine a prognosis, tactics for further examination and treatment of patients in medicine, consultations are traditionally used - meetings of several representatives of one or different specialties. Such consultations, in fact, are examinations - research conducted by a person competent in a certain (usually "narrow") subject area, attracted on behalf of interested parties in order to answer questions that require special knowledge in several subject areas [1-3]. In particular, in accordance with international standards and regulations (GCP, GMP, GLP, etc.), the development of a consensus by a group of experts on a particular issue is the initial level of clinical research based on evidence-based medicine technologies [3-5].
The progress of information and telecommunication technologies made it expedient to implement consultations in the form of network examinations using digital distributed platforms - examinations widely using modern information technologies, communication and data transmission networks for organizing group expert procedures with the involvement of network experts who have equals (including independently from the place of stay) the possibility of participating in the examination [6-9]. Therefore, the development of the architecture of a digital distributed platform for medical consultations is an urgent task.

2. BACKGROUND

The most suitable solution for decentralized automated systems that are used to collect, process, store, transfer and control access to information are architectures based on distributed ledger technologies (blockchain technologies). The use of such technologies for digital distributed platforms of medical consultations protects the processed information from distortion, which ensures the objectivity of the results of the consultations.
Conducting a consultation involves the sequential implementation of the steps [10, 11]:
1) making a decision on the need for a consultation and formulating its purpose;
2) selection and appointment of the composition of the group of specialists: the head (moderator) and the secretary responsible for the technological support of the council;
3) development of the task for the council by the working group (first of all, the scientific supervisor and secretary);
4) development by the working group of a scenario (regulations) for collecting and analyzing expert opinions (assessments) of the participants of the consultation;
5) selection of participants of the consultation in accordance with their specializations and competencies;
6) formation of a group of specialists - participants of the consultation and providing them with the necessary information about the history and current condition of the patient;
7) collecting the opinions of the participants of the council;
8) analysis of the information received using the methods included in the script: when several rounds are used according to the scenario of the council, the necessary repetition of the rounds;
9) final analysis of opinions, interpretation of the results obtained and preparation of the final document;
10) the official end of the consultation, including the approval by the head of the final document, its presentation to the customer of the consultation.

Distributed ledger technologies assume the use of a continuous sequential linked list of blocks containing information in the form of a replicated distributed database [12-15]. The connection between blocks is provided both by numbering and by the fact that each block contains its own hash-sum and hash-sum of the previous block, and changing information in one block leads to the need to edit all subsequent blocks (copies of block chains are stored independently of each other on the set different computers) [16].

The blockchain will allow creating a secure distributed replicated database that unites numerous members of the councils who can track, verify, execute transactions and provide storage of received and processed information. To ensure the security of blockchain technology, many data transfer protocols have been developed and are used, the most common is the node consensus algorithm [17, 18].

To achieve consensus, the blockchain uses many (more than three) distributed network participants: they use their computers to authenticate and verify each new block - for example, to ensure that any one transaction does not go through multiple times. New blocks are accepted by the network as soon as the majority of its participants agree that they are valid [19].

The base publicly stores in encrypted form information about all transactions signed using asymmetric encryption.

According to the type of management and a number of related factors, depending on the characteristics used, the blockchain is divided into three types: open, closed and combined [20, 21].

To ensure the confidentiality of information processed during consultations, it is advisable to create a confidential data transmission network using closed blockchain technology [22].

To hold a consultation using a closed blockchain technology, it is necessary to create a special digital distributed platform of medical consultations in the form of a distributed database for persons participating in the consultation. When passing authorization, experts participating in the consilium can receive signed documents in the form of messages and results of examinations (expert opinions). The process of sending cryptographically signed and authenticated data using closed blockchain technologies ensures the security (confidentiality) of the council and, at the same time, can be checked at any time by designated users (audit nodes) or authorized bodies.

In a closed blockchain, there is no need to verify all operations in each node: all nodes of the blockchain network are trusted, so no significant computational costs are required. The closed blockchain allows specialists from various institutions (organizations) to interact within the framework of a single database within the framework of consultations, which provides significant savings in resources and funds [15, 17, 19].

The costs of providing medical consultations based on closed blockchain technologies are minimal, since it is possible to use existing telecommunications and server equipment. It is possible to give the right to manage the council of external systems (municipal health authorities): this will reduce the required computing power of the participants of the councils. At the same time, complete agreement between the nodes is not required, and to complete any transaction, a smaller number of nodes must perform their functions.

The blockchain functions as a transaction log that records all changes in the state of the system. Operations, collected in blocks, cryptographically linked to each other, form a sequence of chains in which all transactions of the platform of the consultation are recorded. These transactions are sorted in chronological order, allowing the council members to receive reliable information on all changes in the medical history. The result of the consultation is non-cancellable transactions, decentralized agreed by all participants of the consultation.

The chain of transitions allows designated audit nodes using client software to efficiently view data for any period of blockchain operation, both forward and backward, providing the ability to confirm the validity of a data transaction without having to view the full history of the blockchain. The given pointers in the branch chain are cryptographic hashes, while the forward pointers are collective signatures of a group of nodes. Thus, the chain of transitions acts as a necessary cryptographic blockchain structure [17, 21].

Each block in the chain consists of the following data elements: the root hash of the operation tree, containing all transactions in the current block; the root hash of the operation tree, representing the current state of the entire chain; hash of the current block, which acts as a unique identifier for the current block; hash backlink pointing to the previous block; a list of forward and backward links pointing to various blocks in the chain for quick navigation in the chain; list of nodes responsible for processing this block [11-17].

The work that nodes have to do to create a new block is time consuming and computationally intensive. This work will be proof of the work done to calculate the hash of the previous block. The nodes independently monitor each other to ensure that the system data record remains unchanged. All this will reduce the likelihood that two blocks will be executed simultaneously, but such a situation is possible. When this happens, a fork is created in the blockchain: nodes can start building a chain on different branches. To avoid this situation, each node keeps track of all branches, but the nodes will try to extend only the longest branch. In this case, the length of the tree is determined not by the number of blocks, but by the total amount of work that was spent on creating a branch and is determined by the number of zeros at the beginning of the hash block.

The computational complexity of transaction verification helps to avoid dependence on the number of nodes in the network that may be subject to unauthorized changes: only the total computing power of the nodes affects the verification. Consequently, for unauthorized change of information in the block, significant computing resources are required, which makes this practically impossible. Since copies of the blockchain are stored in the nodes of the digital distributed platform: this makes the platform resistant to problems with temporary or permanent disconnection of nodes associated with equipment failures or communication channels, as well as the connection of new nodes [14, 17, 18].

The Consensus Execution Module on a Digital Distributed Platform consists of a set of consensus nodes that collectively validate the operations (actions) performed. Transactions can consist of various elements of a consensus, including voting forms, a configuration file, and a consensus confirmation. Any of the consensual nodes is referred to as a "full node" [13]. "Full nodes" are the nodes of a digital distributed platform that store all information about all transactions on the network. The "full node" node receives the expert vote and other data from the consensus nodes, proposes the creation of new information blocks, and writes the confirmed blocks to the log. Nodes and consensus nodes in the network can be used by independent auditors [15, 22].

Consensus nodes serve the following purposes: maintain a copy of the blockchain; receive encrypted guidelines from the head of the council and participate in the authentication of these data, ensure the sending of the results of the councils and surveys of authorized specialists; confirm blocks provided by the database server; decipher the polls of experts after the end of voting, create an open vote, form the final data; keep copies of the journal and check its correctness.

To increase the speed of search and control over transactions, the platform uses additional long communication lines between them [17].

The usual list of transactions should be supplemented by one or two linked lists, but the use of additional communication lines, which are structurally redundant, allows much more efficient use of the search for transactions on them in the timeline using logarithmic rather than linear steps.

To adapt the idea of skipping locks, additional long lines of communication are used, which are added both forward and backward.

The developed architecture of the digital distributed platform of medical consultations in the form of a blockchain network combines nodes (workstations connected to the blockchain network) with write permissions, managed by the council leader and recognized external consensus nodes, as well as nodes with read-only permissions (audit nodes) , in the role of which there can be automated workstations of the participants of the council. This blockchain network provides an immutable record of all data in platform nodes throughout the network and acts as a central communication channel and storage for the entire system.

A digital distributed platform is a distributed database for specialists participating in a consilium, to which, when authorized, a consilium member can send signed data in the form of messages and voting results. The process of sending cryptographically signed and authenticated data is stored in the blockchain - thus, the entire consultation process on the platform becomes secure, private and can be checked at any time by designated users (audit nodes).

Storing copies of the blockchain in the nodes of a distributed network makes the platform resistant to problems with temporary or permanent disconnection of nodes associated with equipment or communication failures, as well as with the connection of new nodes.

3. CONCLUSION

Thus, the proposed solution will allow validating a reference block using cryptographically validated tokens that represent a large group of hashes of adjacent blocks. The end result is that even platform users (councilors) with limited resources, such as low network bandwidth, can receive and efficiently check binary updates using a hard-coded initial version of the software as a trust anchor. Such platform nodes do not need to constantly monitor the chain of information block creation, as bitcoin does in a full node, but can privately exchange data and independently check autonomously necessary blocks by forward and backward links.

The implementation of technologies to support medical diagnostic decisions using consultations organized on the basis of digital distributed platforms is one of the priority tasks of medical informatics. Despite the obvious advantages, the implementation of such approaches is associated with the need to solve problems that allow implementing an effective network expertise. The solution of these problems, undoubtedly, requires the joint efforts of specialists in computer science, management, computer technology, information security, psychology, sociology, etc., as well as close attention of society.

Thus, the proposed method of organizing the chains of transitions when holding consultations in a closed blockchain will allow creating a secure distributed platform for holding consultations, consisting of an expert community.

Authorized bodies that control the quality of medical services will be able to reliably track, verify transactions and ensure the safe storage of information about the network expertise. By implementing the idea of skipping locks, the problem of quick access to the actual protected information necessary for the work of remote participants of the council was solved. At the same time, the possibility of third-party interference and data distortion will be minimal.

ACKNOWLEDGMENT

The study was carried out with state support from leading scientific schools Russian Federation, grant No. NSh-2553.2020.8.

REFERENCES

[1] M. Bode, Towards a Formal Description Language for Digital IT Consulting Products in Decentralized IT Consulting Firms, IEEE 23rd International Enterprise Distributed Object Computing Workshop (EDOCW), Paris, France, 2019, 168-173. DOI: 10.1109/EDOCW.2019.00037.

[2] R.W. White, S T. Dumais, J. Teevan, How medical expertise influences web search interaction, Proceedings of the 31st annual international ACM SIGIR conference on Research and development in information retrieval, 2008, 791-792. DOI: 10.1145/1390334.1390506

[3] D. Murugadas, S. Sizov, Do it yourself diagnosis: a study on acquiring health-related information online, Proceedings of the 8th ACM Conference on Web Science, 2016, 276-285. DOI: 10.1145/2908131.2908147

[4] A.I. Maistrou, A.V. Bogomolov, Technology of automated medical diagnostics using fuzzy linguistic variables and consensus ranking methods, World Congress on Medical Physics and Biomedical Engineering: Diagnostic and Therapeutic Instrumentation, Clinical Engineering, Munich (2009) 38-41. DOI: 10.1007/978-3-642-03885-3-11

[5] N.D. Silverberg, G.L. Iverson, D.B. Arciniegas, M.T. Bayley, J.J. Bazarian, K.R. Bell, Expert Panel Survey to Update the American Congress of Rehabilitation Medicine Definition of Mild Traumatic Brain Injury, Archives of Physical Medicine and Rehabilitation, 2020. DOI: 10.1016/j.apmr.2020.08.022

[6] D. Perepelkin, A. Gostin, A. Saprykin, M. Ivanchikova, S. Kosorukov, Development of Digital Platform Architecture of Distributed Data Processing, 8th Mediterranean Conference on Embedded Computing (MECO), Budva, Montenegro, pp. 1-5, 2019 DOI: 10.1109/MECO.2019.8760173

[7] E.V. Larkin, A.V. Bogomolov, A.N. Privalov, N.N. Dobrovolsky, Relay races along a pair of selectable routes, Bulletin of the South Ural State University Series-mathematical Modelling Programming & Computer Software, 11(1) (2018) 15-26. DOI: 10.14529/MMP180102

[8] O.A. Slavin, Recognition algorithms for structured documents with variable composition, Programming, 31 (4) (2005) 63-80

[9] E.V. Larkin, A.N. Privalov, A.V. Bogomolov, Discrete approach to simulating synchronized relay races, Automatic documentation and mathematical linguistics, 54(1) (2020) 43-51. DOI: 10.3103/S0005105520010082

[10] A.G. Chkhartishvili, D.A. Gubanov, N.A. Korgin, D.A. Novikov, Models of reputation dynamics in expertise by social networks, UKACC International Conference on Control, Coventry, 2010, 1-8. DOI: 10.1049/ic.2010.0281

[11] A.V. Bogomolov, R.S. Klimov, Automation of information processing during collective network examinations, Automation. Modern technologies, 71 (11) (2017) 509-512

[12] N. Kefalakis, A. Roukounaki, J. Soldatos, A Configurable Distributed Data Analytics Infrastructure for the Industrial Internet of things, 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, pp. 179-181, 2019. DOI: 10.1109/DCOSS.2019.00048

[13] T.M. Fernández-Caramès, F.P. Towards, Post-quantum blockchain: a review on blockchain cryptography resistant to quantum computing attacks, IEEE Access, 8 (2020) 21091-21116. DOI: 10.1109/ACCESS.2020.2968985

[14] E.V. Larkin, A.V. Bogomolov, A.N. Privalov, N.N. Dobrovolsky, Discrete model of paired relay-raceweb of science, Bulletin of the South Ural State University Series-mathematical Modelling Programming & Computer Software, 11(3) (2018) 72-84. DOI: 10.14529/MMP180306

[15] A. Brinckman, A comparative evaluation of blockchain systems for application sharing using containers, 13th International Conference on e-Science. Auckland, pp. 490-497, 2017. DOI: 10.1109/eScience.2017.80

[16] S. Sultan, I. Ahmad, T. Dimitriou, Container security: issues, challenges, and the road ahead, IEEE Access, 7 2019, 52976-52996. DOI: 10.1109/ACCESS.2019.2911732

[17] D.S. Tobin, Peculiarities of the organization of transition chains when conducting network examinations in a closed blockchain, I-methods, 12(2) (2020) 1-10

[18] M. Belotti, N. Božić, G. Pujolle, S. Secci, A vademecum on blockchain technologies: when, which, and how, IEEE Communications Surveys & Tutorials,

21(4) (2019) 3796-3838. DOI: 10.1109/COMST.2019.2928178

[19] K. Lei, M. Du, J. Huang, T. Jin, Groupchain: Towards a scalable public blockchain in fog computing of iot services computing, IEEE Transactions on Services Computing, 13(2) (2020) 252-262. DOI: 10.1109/TSC.2019.2949801

[20] S. Kwon, J. Lee, DIVDS: docker image vulnerability diagnostic system, IEEE Access, 8 (2020) 42666-42673. DOI: 10.1109/ACCESS.2020.2976874

[21] D.S. Tobin, Network expert-analytical platform as a tool for decision support in a distributed environment, Vestnik NSUEU, 3 (2020) 231-240

[22] S.K. Lo, Y. Liu, S.Y. Chia, X. Xu, Q. Lu, L. Zhu, H. Ning, Analysis of Blockchain Solutions for IoT: A Systematic Literature Review, IEEE Access, 7 2019, 58822-58835. DOI: 10.1109/ACCESS.2019.2914675