**Yu. V. Baryshev, Cand. Sc. (Eng.), Associate Professor; V. S. Lanova**

# METHOD OF THE PROTECTED STORAGE OF MEDICAL DATA, BASED ON THE RELATIONAL DATABASE AND BLOCKCHAIN

*The paper contains the analysis of the known practices of using the blockchain technology in the health care sphere. Structures of the data storage organization have been considered. Tasks, emerging in the process of blockchain technology application for storage of the confidential information in critical systems, such as, medicine are determined. The paper contains the analysis of the system of creation of the electronic medical referrals, used in Ukraine. Method of medical data storage, based on the usage of the hybrid storage environment, based on the blockchain and relational data base has been suggested. The basis of the method is the classification of the data according to the requirements regarding the security of the information properties, the reflection of which these data are, for the determination of their storage method. To prove the usability of the method the example of its realization for the problems in the sphere of family medicine, namely, the process of issuing of electronic referrals for the additional health examination by the specialists, is presented. The results of projecting the relational data base for this subject field are shown, within the limits of this projecting main essences and attributes of this data base are determined. The analysis of the requirements, regarding the security of these data has been carried out, on the base of the analysis their classification according to the suggested method has been performed. For storage of the data in the blockchain, corresponding smart-contract has been developed, it provides the interface for the access of the data, which require improved integrity security, accessibility and combination of these properties. Programming module for combining the relational data base and blockchain to reflect the data for clients programs incapsulated, irrespective of the actual place of their storage, has been developed. Mechanism for improving the security of the data integrity in the relational data base at the expense of their verification in the blockchain, without disclosing the content of these data has been suggested. Perspectives of further research are defined.*

***Key words:*** *cyber security, data base, blockchain, medical secret, personal data, family doctor, smart-contract, critical systems.*

## Introduction

Medical data security is obvious: according to the legislation they are part of medical secrecy [1] and personal data [2 – 3]. At the same time these data may be used in the process of incidents investigation, that is why, their integrity and accessibility is critical for the successful investigation of both medical errors or clinical negligence and their protection from the groundless charges on the part of patients or the state organs. In this case the medical data must be transparent and at the same time they must be protected against the unauthorized access.

Accordingly, the solution of the problem of the medical data security provides the usage of the specialized methods of their storage and processing as well as special data structures, which will allow to realize it. Possible solution of this problem can be blockchain technology. This technology suggests new approaches to the model of storage and management of the data, used nowadays in many programs in the health care sphere. This is connected with the ability to segment and protect the integrity and accessibility of the information. At the same time the openness of the blockchain for the access generates problems for confidentiality protection. Besides, usage of only the blockchain technology for data storage requires more resources for the creation and support of the unit of information storage as compared with the conventional databases. That is why, there appears the relevant problem, dealing with the development of the method of storage, which will enable to combine the advantages of these technologies for the critical systems such as health care.

**Objective of the given research** is to improve the medical data protection by developing the method of their separate storage on the base of relational data base and blockchain, which supports the smart-contracts.

To achieve the set objective the following problems are to be solved:

– carry out the analysis of the known methods of the blockchain technology application of storing medical data;

– develop the method for the organization of the secured data storage;
– analyze the subject area;
– develop the data model;
– develop smart-contracts, which will store data in the blockchain.

For the concept proof the given paper contains the information, processed during issuing the referrals, needed for the additional examination by the family doctors.

### Analysis of the known methods of blockchain technology application for medical data

Natural state for the data, stored in blockchain is their openness. This is stipulated by the technology distribution and permanent exchange of the information between the nodes. That is why, the research, aimed at protection of the data confidentiality is carried out. In particular, in the study [4] the mechanism of privacy protection for the data distribution among the patients, doctors and providers of medical services is considered. The approach, suggested by the authors [4] provides the usage of pseudonyms in the process of data exchange for the protection of the patients` privacy. This method also takes into account the peculiarities of medical system and legislation of Sweden, in particular, control of the approval of the decisions, regarding the volume of data, that complicates the implementation of the suggested technologies of obtaining the access in the conditions of the legislation base of other countries.

Wide application of the blockchain technology in medical sphere is observed in Estonia [5]. Every citizen of this country, who visited the doctor, has on-line record in the E-Health system, this record can be monitored by all state medical institutions [5]. Usage of the blockchain technology in the system provides the integrity of the data and softens the internal threats for the data. However, the drawback of this system is that for recording of all the data large volume of the resources is needed: great number of transactions are to be carried out, this causes the computational resources consumption .

Authors [6] propose to use the blockchain for adding medical data. After the patient visits the hospital, the doctor make diagnosis and creates the health card. The doctor has to save the records to give the possibility for the patient to address his data and the doctor will have the possibility to learn the details. As the medical records are connected with the personal data of the patients, before saving the data must be coded. The doctor codes and signs medical documentation, then he loads it into IPFS system [7] for storage and generates indices for the key words. IPFS gives back hash-address of the saved file to the doctor. After that, having received hash-addresses, the doctor codes and hashes medical documentation and its index by means of SHA-256 and saves hash value and coded hash-address in the blockchain [6].

The research [8] presents the architecture of the control system to medical data access, stored in the blockchain, on the base of the role model of the access rights differentiation. In particular, the research provides state regulation regarding the policy of the access rights differentiation and feed back system from the patients and administrators of the information systems (Fig. 1).

The drawback of the approach, suggested in [8] is its concentration, concerning data storage, exclusively on the blockchain, this decreases the data access speed. Besides, lack of data security, integrated directly into the blockchain, causes the growth of the human factor impact on the process of the access rights differentiation.

Authors of the study [9] suggested the approach to the solution of the problem of medical data storage in the blockchain on the base of usage the model of access right differentiation and data coding. Main advantage of this approach is the usage of coding for the protection of the confidentiality but at the same time coding complicates the procedure of the key transport. Taking into account a great number of the parties involved (patients, doctors, organs of the state regulation, scientists-researchers, etc.), the problem of the keys distribution among a great number of the participants generates additional problems, which need further study.

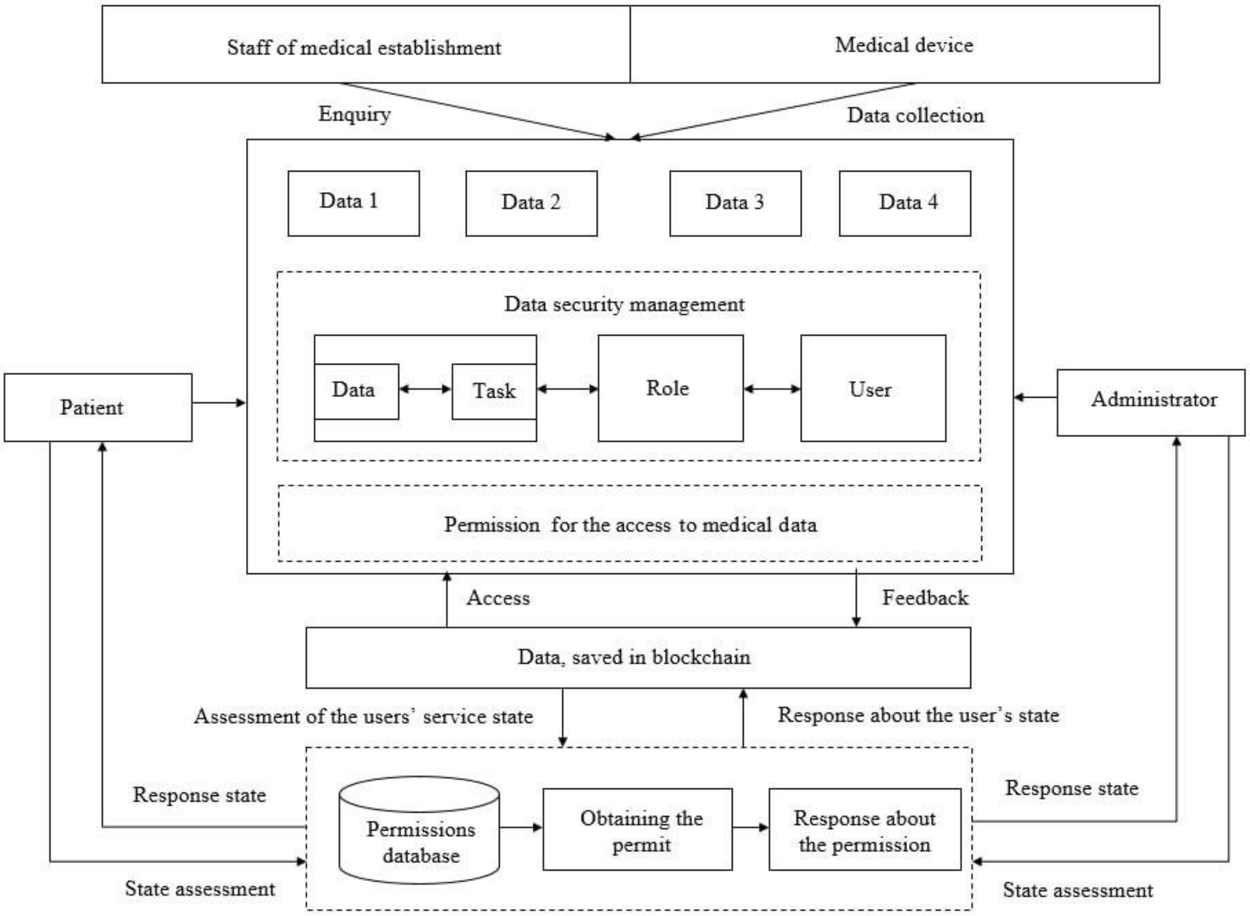


Fig. 1. Architecture of the blockchain-based system of medical data access control

The study [10] is based on the deployment of the private blockchain on the base of the code system of Ethereum blockchain. Since the basic unit of data structuring in Ethereum is smart-contracts, they are used for storing the information, contained in the electronic medical card of the patient, which contains personal data. During the processing of the data it is important to take into consideration their security. For this purpose the authors developed the model for medical data exchange between the patients, doctors and any other establishment, participating in this procedure. The smart-contracts, used provide confidentiality of the electronic medical cards of the patients by means of cryptographic functions and access control functions. Application of the private blockchain limits the accessibility protection of the data, stored in it. However, in the sphere of the health care information accessibility is critical, for instance, in cases of the urgent medicine.

In the paper [11] the construction of the blockchain for storing medical data on the base of smart-contracts and sharding is considered. For data protection the authors [11] suggest the technology of data noise masking and development of smart-contracts, which will manage the data processing. Accordingly, the systems in health care establishments and clients facilities will interact with the smart-contracts for changing the state of the blockchain. The drawback of data noise making is the growth of the data sets, which are to be stored in the blockchain, for which high level of the data backup is general drawback.

Medical system of Ukraine is in the process of the reforming and modernization. Ministry of Health of Ukraine by the order of June 9 2017 № 17 approved the regulation of e-system of the health care functioning within the frame of the pilot project in the part of provision of the automation of medical services accounting [12]. One of the main directions of this regulation is the implementation of e-Health system, the aim of which is the improvement of the efficiency and transparency of the health care system.

Health care electronic system (HCES) – is two component system, where the user interacts with the central data base via medical information system [13].

HCES consists of such elements [13]:

– central data base of information-telecommunication system, it contains registers, programming modules, information system of National health care service of Ukraine, etc.;

– electronic medical information system – information-telecommunication system, enabling to automate the operation of the entities in the field of healthcare, create, look trough, exchange information in electronic form, in particular, with the central data base.

Right of access to the personal data of the patients in the sphere of the healthcare have the following persons: medical staff or other persons of the health care establishment; sole proprietors, practicing medicine on the base of the license; persons, covered by the legislation on medical confidentiality; officials of the central government bodies, realizing the state policy in the sphere of the state financial assurance of public health service [14]. Such wide spectrum of persons involved complicates the management of the access distribution as it requires the determination of the access rights for each party.

Besides, the availability of the central data base generates a single point of failure of the whole system, that generates a number of threats to the integrity and accessibility of the information. Thus, the analysis proves the need of using the blockchain hybridization with other data storage technologies. As in the critical systems such as medicine, the number of users and volume of data to be processed, require the possibility of scaling. At the same time, the blockchain by its nature is inflexible and cannot be considered an adequate tool for data storage in such problems.

## Method of data vaulting

As it was shown in the previous section – modern state of the development of methods for medical data storage in the blockchain is not adapted to the realities of medical practice and documents circulation in Ukraine. Nowadays as the system of electronic circulation of documents has been used, the proposed solution must take into account the possibility of gradual transition to the usage of blockchain. Besides, the property of the openness and low level of blockchain scalability stipulates along with advanced level of the integrity security, loss of data confidentiality in case if they are published in the open form. That is why, the method of medical data storage, based on the combination of the conventional relational data bases, used in the current practice, with the blockchain is suggested.

The suggested method provides the following steps:

Step 1. Analysis of the subject area, collection of the relevant data and its further formalization in the form of the attributes of the data base.

Step 2. Normalization of the data base relations.

Step 3. Analysis of the requirements to each attribute in the obtained normalized data base from the point of confidentiality and integrity. As a result of the analysis all the data is distributed in the following classes:

– data, which does not need the advanced protection;

– data, requiring the advanced protection of the integrity (I);

– data, requiring the advanced protection of the accessibility (A);

– data, requiring the advanced protection of the confidentiality (C);

– data, requiring the advanced protection of several properties at the same time (IA, CI, CA, CIA).

Step 4. Development of the smart-contracts for transfer data of I, A and IA categories into the blockchain with introducing modifications.

Step 5. Development of the containers for the protected storage of the data of CA category on the base of the method of detection and correction of the errors.

Step 6. Development of the containers for the protected storage of CA data on the base of the coding methods.

Step 7. Development of the containers for the protected storage of CIA data on the base of the methods of coding, detection and correction of the errors.

Step 8. Introduction into the relational base the data of new attributes with the information about the reference to the smart-contract, where the data were transferred.

The suggested method enables to distribute the data among the data base and blockchain, using the blockchain only for the protection of the data, which requires the advance protection of the integrity and accessibility. Unlike the known methods, in particular, those which were considered in the previous section of the paper, this method provides the simultaneous access of a large number of the parties involved, as it is common for medical sphere. In this case, the complexity of the task of the access rights distribution management decreases due to the allocation of the data, which require access limitation and storage in the separate containers.

## Application of the method for medical data

To prove the concept, family medicine, namely, the process of obtaining the direction for the additional examinations at the hospital has been chosen. Introduction of the blockchain may provide high level of the patients data security, provide authenticity and will make impossible any changes in the records as well as will promote the transparency and traceability of medical services. Such an approach will improve the efficiency of medical processes management in the sphere of family medicine.

On the base of the subject field analysis, carried out, basic entities of the data base and their attributes were allocated. For further study the real referral to otolaryngologist, issued on 10.08.2022 in the Center of primary care №2, Vinnytsia was taken, the referral contains:

– № of the referral  – unique identifier of the referral ;
– specialist – doctor who created the referral;
– name of the examination or procedure;
– name of the patient – full name of the patient;
– provisional diagnosis – provisional medical diagnosis of the patient;
– date of the referral  issue – date, when the referral  was created;
– priority – degree of importance or urgency of the examination;
– expiration time – term, during which the appointment is valid;
– № of medical card of the patient – unique identifier of medical card of the patient;
– service code – unified code of the examination or procedure;
– № of the doctors certificate – unique identifier of the doctor, who created the referral ;
– name of medical establishment – name of the hospital or medical establishment;
– ЄДРПОУ/РНОКПП – code – identification code of medical establishment, according to the registers.

These attributes form complex system of the monitoring and control over the provision of medical services in the sphere of family medicine in the hospital. According to previously allocated attributes, the analysis of the given data is carried out. The results of the analysis are presented in Table 1.

Table 1

**Analysis of the given attributes**

| Attribute | Protection of confidentiality | Protection of the integrity | Protection of the accessibility |
|---|---|---|---|
| № of the referral | - | + | + |
| Specialist, to whom the referral was directed | + | + | + |
| Name of the examination | + | + | + |
| Full name of the patient | + | - | - |
| Previous diagnosis | + | - | - |
| Date of the referral  issue | - | - | - |
| Priority | - | - | + |
| Validity term | - | - | + |
| № of medical card of the patient | + | + | - |
| Code of service | - | - | - |
| № of doctor passport | + | + | - |
| Name of the health care establishment | - | + | - |
| Code by ЄДРПОУ/РНОКПП | - | - | + |

For this subject field data base under the name MedicalData has been  developed. Basic table of the data base is _MedicalRecords, containing such fields:

– patientName,

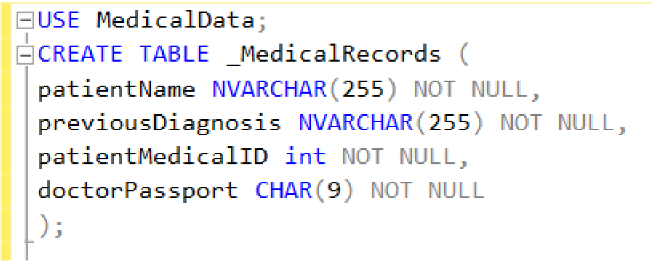
– previousDiagnosis,

– patientMedicalID,

– doctorPassport.

These fields store full name of the patient, diagnosis, identification number of the patient (or № of medical card) and № of doctor passport, correspondingly.

This Table is created taking into account the requirements of medical data confidentiality and easy access for medical personal. For its realization the request was developed (Fig. 2).

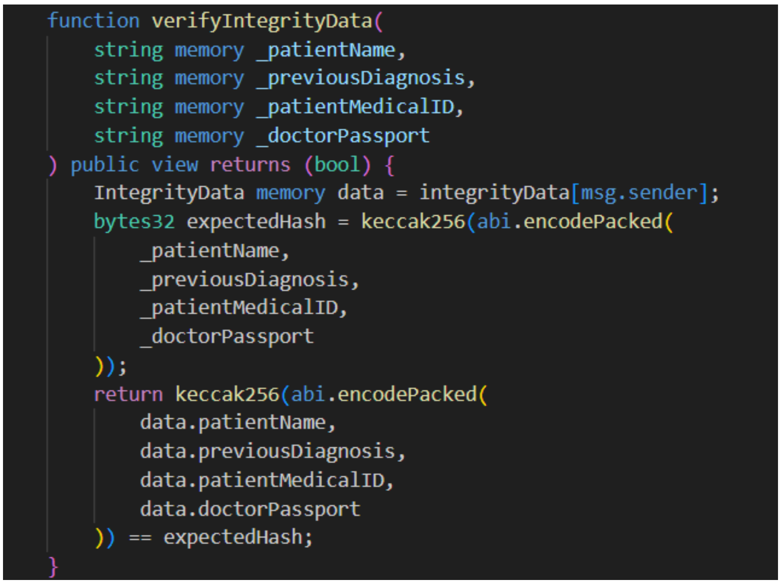


```
USE MedicalData;
CREATE TABLE _MedicalRecords (
patientName NVARCHAR(255) NOT NULL,
previousDiagnosis NVARCHAR(255) NOT NULL,
patientMedicalID int NOT NULL,
doctorPassport CHAR(9) NOT NULL
);
```

Fig. 2. Request for the creation of the Table

Each of four fields of the Table is obligatory and must not be empty. This enables to avoid the incomplete or incorrect records. The obligatory character of MedicalRecords table fields excludes the possibility of adding incomplete or incorrect records in the data base, providing the advanced level of data protection.

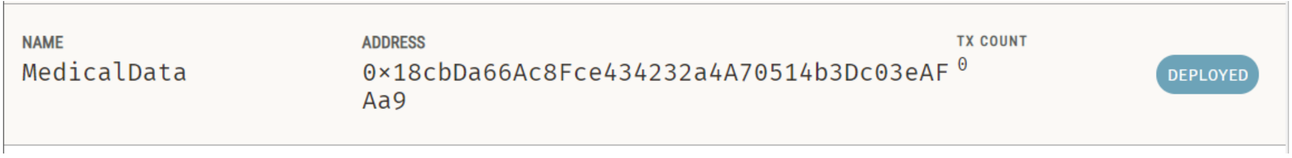
Besides the data base smart-contract has been developed, it serves as a base for storage the data, requiring the advanced level of the integrity protection and accessibility to the information. For smart-contract realization Solidity language is used. For the distribution of the access to the data with different requirements regarding protection level, separate groups of functions which enable to read and add such categories of data as I, A and IA were developed. For the interaction with last group of functions additional verification of data integrity was developed. For this purpose hash-function keccak256 is used, which is supported by the blockchains of Ethereum family. The obtained hash-values are written into the blockchain, that enables to improve their protection against falsification. Further, it is provided to compare these hash-values with the calculation of hash-values of the data, stored in the data base, this enables to reveal cases of unauthorized modification of the data base (Fig. 3).



```
function verifyIntegrityData(
    string memory _patientName,
    string memory _previousDiagnosis,
    string memory _patientMedicalID,
    string memory _doctorPassport
) public view returns (bool) {
    IntegrityData memory data = integrityData[msg.sender];
    bytes32 expectedHash = keccak256(abi.encodePacked(
        _patientName,
        _previousDiagnosis,
        _patientMedicalID,
        _doctorPassport
    ));
    return keccak256(abi.encodePacked(
        data.patientName,
        data.previousDiagnosis,
        data.patientMedicalID,
        data.doctorPassport
    )) == expectedHash;
}
```

Fig. 3. Fragment of the code for revealing the unauthorized modification of the data base

The developed smart-contract is deployed in Ethereum-like network by means of Ganache environment (Fig. 4).



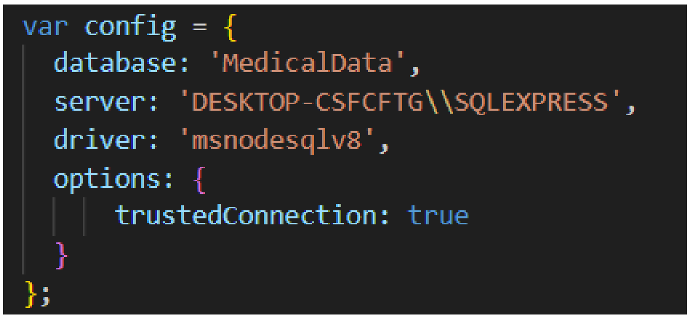
| NAME | ADDRESS | TX COUNT | |
|---|---|---|---|
| MedicalData | 0x18cbDa66Ac8Fce434232a4A70514b3Dc03eAFAa9 | 0 | DEPLOYED |

Fig. 4. Result of the smart-contract deployment

The next task is the development of the software, which will enable to interact simultaneously with the data, stored in the data base and in blockchain, as with a single source of data.

## Connection of the data base to the blockchain

For the development of the program of data base and blockchain integration ethers.js library was used. Programming module, which performs the connection of the data base to smart contract was elaborated. First, the connection of the data base to program application in the environment node.js was carried out. For this, purpose, the configuration of the connection, shown in Fig. 5 was carried out.



```
var config = {
  database: 'MedicalData',
  server: 'DESKTOP-CSFCFTG\\SQLEXPRESS',
  driver: 'msnodesqlv8',
  options: {
      trustedConnection: true
  }
};
```

Fig. 5. Configuration file for data base SQL Server connection

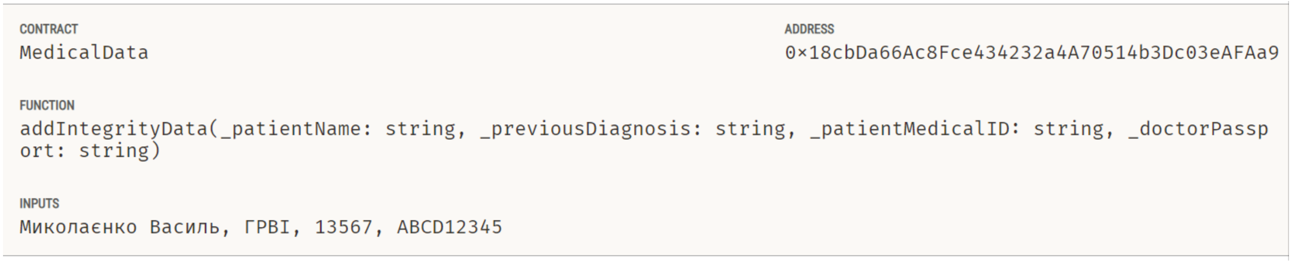
Integration of the data base into the deployed smart-contract during data adding is realized in the following way:

– address of the contract is obtained;

– SQL-enquiry is formed in the environment node.js, which performs recording into the data base;

– record into the blockchain takes place .

Further after the successful start and connection, data, added both into the blockchain and data base can be seen (Fig. 6 – 7).

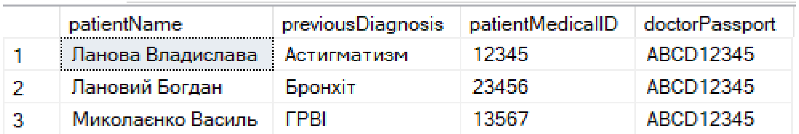


```
CONTRACT                                          ADDRESS
MedicalData                                       0x18cbDa66Ac8Fce434232a4A70514b3Dc03eAFAa9

FUNCTION
addIntegrityData(_patientName: string, _previousDiagnosis: string, _patientMedicalID: string, _doctorPassp
ort: string)

INPUTS
Миколаєнко Василь, ГРВІ, 13567, ABCD12345
```

Fig. 6. Representation  of the successful data adding into the blockchain



| | patientName | previousDiagnosis | patientMedicalID | doctorPassport |
|---|---|---|---|---|
| 1 | Ланова Владислава | Астигматизм | 12345 | ABCD12345 |
| 2 | Лановий Богдан | Бронхіт | 23456 | ABCD12345 |
| 3 | Миколаєнко Василь | ГРВІ | 13567 | ABCD12345 |

Fig. 7. Representation of the successful adding of the records into the data base

Reading of the information takes place according to the analogous principle. In the process of reading of the data from the blockchain the transactions should not be performed, this provides higher speed of reading as compared with recording.

## Conclusions

Analysis of the known practices of the blockchain application in medicine in different countries showed complex problems dealing with the integration of these methods in medical sphere of other countries due to the differences of the legislation, regulating the rules of documents circulation. Besides, for medical sphere it is important to provide simple architecture and management of complex development. That is why, the authors suggested the method, which enables to perform the classification of the data according to the requirements of the protection of the confidentiality, integrity and accessibility of data. This allowed to create various containers (data base or smart-contracts), protected by different protection methods, depending on the properties of the information, the given container is intended for. Thus, all the data of the subject field, which have similar requirements to the information protection are stored within the limits of one container. Unlike the known approaches, this enabled not to apply the methods of information protection to the data, which do not need to be protected. This promotes more efficient distribution of the computational resources and improves the scalability of the information system on the base of such method of data storage. The latter is very important for critical systems such as medical ones, as the characteristic feature of these systems is long storage of data and growth of the volume of these data along with the increased duration of the information systems usage for the automation on business-processes in these fields.

To prove the efficiency of the suggested method the example of its realization in the sphere of medical practice of family doctors, namely, registration of the referrals for the additional examination is considered. Mechanism of the data base integrity improvement as a result of their verification in the blockchain without disclosing the data content is suggested.

## REFERENCES

1. Law of Ukraine ” Fundamentals of the legislation of Ukraine on health care [Electronic resource] : Law of 19.11.1992 № 2801-XII: as of 24 September 2023 (valid) – Access mode : https://zakon.rada.gov.ua/laws/show/2801-12 (date of access: 24.09.2023). – Name from the screen. (Ukr.).

2. General Data Protection Regulation (GDPR) – Official Legal Text [Electronic resource] // General Data Protection Regulation (GDPR). – Mode of access: https://gdpr-info.eu/ (date of access: 04.09.2023).

3. Law of Ukraine “ On personal data protection [Electronic resource] : Bulletin of Verkhovna Rada of Ukraine, 2010, № 34, p. 481: as of 24 September 2023. (valid) – Access mode : https://zakon.rada.gov.ua/laws/show/2297-17 (data of access : 24.09.2023). (Ukr.).

4. Accessing and sharing health information for post-discharge stroke care through a national health information exchange platform - a case study [Electronic resource] / N. Davoody, S. Koch, I. Krakau, M. Hägglund // BMC Medical Informatics and Decision Making. – 2019. – Vol. 19, № 95. – Mode of access: https://doi.org/10.1186/s12911-019-0816-x (date of access: 25.09.2023).

5. e-Health Record – e-Estonia [Electronic resource]. – Mode of access: https://e-estonia.com/solutions/healthcare/e-health-records/(date of access: 27.09.2023).

6. Blockchain-Based Secure Storage and Access Scheme For Electronic Medical Records in IPFS [Electronic resource] / J. Sun, X. Yao, S. Wang [et al] // IEEE Access. – 2020. – Vol. 8. – P. 59389 – 59401. – Mode of access: https://doi.org/10.1109/access.2020.2982964 (date of access: 25.09.2023).

7. Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web [Electronic resource] / D. Trautwein, A. Raman, G. Tyson [et al] – Mode of access: https://doi.org/10.1145/3544216.3544232 (date of access: 25.09.2023).

8. Data Access Control Based on Blockchain in Medical Cyber Physical Systems [Electronic resource] / F. Chen, J. Huang, C. Wang [et al] // Security and Communication Networks – Mode of access: https://doi.org/10.1155/2021/3395537 (date of access: 25.09.2023).

9. A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection [Electronic resource] / Y. Chen, L. Meng, H. Zhou [et al] // Wireless Communications and Mobile Computing. – 2021. – Vol. 2021. – P. 1 – 12. – Mode of access: https://doi.org/10.1155/2021/6685762 (date of access: 20.09.2023).

10. A Smart Contract Based Access Control Framework for Cloud Smart Healthcare System [Electronic resource] / A. Saini, Z. Qingyi, Y. Xiang // IEEE Internet of Things Journal. – 2020. – P. 1. – Mode of access: https://doi.org/10.1109/jiot.2020.3032997 (date of access: 25.09.2023).

11. Artificial Neural Network Blockchain Techniques for Healthcare System: Focusing on the Personal Health Records [Electronic resource] / Seong-Kyu Kim, Jun-Ho Huh // Electronics. – 2020. – Vol. 9, № 5. – P. 763. – Mode of access: https://doi.org/10.3390/electronics9050763 (date of access: 25.09.2023).

12. Rules of functioning of electronic system of Health care in framework of implementation of the pilot project in the part of provision of the automation of health care provision record [Electronic resource] : order of Public Health Ministry of Ukraine of 09.06.2017. Access mode : https://www.apteka.ua/article/415112 (data of access: 25.09.2023). (Ukr.).

13. E-Health [Electronic resource]. – Access mode : https://ehealth.gov.ua/ (date of access : 25.09.2023). (Ukr.).

14. E-Health : mechanism of implementation and stages of development [Electronic resource] / N. V. Korobtsova // Legitimacy problems. – 2021. – Issue 154. – P. 117 – 126. – Access mode : https://doi.org/10.21564/2414-990X.154.236921 (date of access: 25.09.2023). (Ukr.).

Editorial office received the paper 22.09.2023.
The paper was reviewed 28.09.2023.

***Baryshev Yuriy*** – Cand. Sc. (Eng.), Associate Professor with the Department of information security.

***Lanova Vladyslava*** – Student with the Department of information security.
Vinnytsia National Technical University.