ACTA SCIENTIFIC MEDICAL SCIENCES

Volume 2 Issue 9 December 2018

Research Article

The Use of Blockchain Technologies and Cryptography Methods in Medicine and Healthcare

Makarov Anatoly*, Pisarenko Elena and Bagdasaryan Serj

Department of Information and Communication Technologies, Mathematics and Information Security; Pyatigorsk State Linguistic University, Russia

***Corresponding Author:** Makarov Anatoly, Professor, Department of Information and Communication Technologies, Mathematics and Information Security; Pyatigorsk State Linguistic University, Russia.

Received: October 25, 2018; **Published:** November 13, 2018

Abstract

To ensure the information security of medical data of patients, the integrity of this data, the simultaneous availability of their medical facilities and privacy, it is necessary to develop an effective technology for managing information security and protecting the information contained in electronic medical records (EMR). This technology should provide such a mode of functioning of medical institutions so that the information already recorded in the EMR cannot be falsified, replaced, spoiled and unauthorized authentication of personal data conducted.

Keywords: Blockchain Technologies; Cryptography Methods; Medicine; Healthcare

Introduction

The order of magnitude of the medical data about a person is doubled every three years. In turn, the update of hardware and software in health care is not keeping pace with the dynamics of data growth. This fact led to the development of the unique IBM Watson system, which was so named after its creator Thomas Watson. This system, as an analytical platform, conducts the following functional stages [1]:

1. Research question;
2. Primary search and hypothesis generation;
3. Filtering the results;
4. Selection of facts and analysis of their quality;
5. Combining results and their evaluation.

At the same time, the tasks of identifying the role of genetic factors in the diagnosis of oncological and rare pathologies are successfully solved [1,2]. The system helps dermatologists identify various skin diseases with a probability of 0.94. The high results obtained in the described case are explained by the presence of reliable initial data at the stage of primary search and generation of hypotheses. But at the same time, it is necessary to simultaneously ensure the preservation of the privacy of the patient's personal data. Since the primary patient data in many countries, for example, in England, USA, Germany, is contained in electronic medical records (EMR), which contain data from both the patient and his family, the medical history from other doctors and insurers, the provision reliability of data, their integrity, impossibility of falsification and privacy is the most important factor in the implementation of all five stages given above.

For example, in 2014, Chicago [2] launched a project to analyze medical records, genetic tests, case histories of patients' relatives in order to detect diseases.

Currently, the technologies of "smart" cities are rapidly developing. For example, in Russia, by 2024, the population of smart cities is expected to be 50 million people. They should include such technologies as remote blockchain technology in energy management and housing and communal services, city management based on digital platforms, artificial intelligence technology in environmental monitoring, as well as in medicine and telemedicine. In the latter case, you need the latest technology in the systems:

- Latest version of mobile 5G communication system (on 2018)- it will reduce the time of data transfer;

- The Internet of Things (IoT) - it will allow doctors to track the health of the population and patients, regardless of their location.
- Big data and their analysis - it will allow you to study the patient more fully and diagnose him, as well as to make the transition from reactive to preventive medicine.
- Artificial intelligence - it will allow to detect diseases at an early stage on the basis of reliable primary data and subsequently to cure it properly. At the same time, it will also allow the doctors to develop and recommend to the doctors, based on the analysis of diagnostic data, possible treatment options.
- Virtual (VR) and additional reality (AR) - it will help the nurse find the patient's vein for drug administration, see the patient's internal organs through the tissue, and VR and AR are important in treating autism, epilepsy or phobias.

The relevance of information technologies is confirmed by the introduction of radio frequency marking on medical electronic cards in Russia, i.e. RFID tags that will be used to track the movement of records outside of the record storages [3,4]. That is, having received a card while receiving a patient, the doctor can use the tag to determine the current location of the card and trace the history of its movement [3]. But, nevertheless, despite the institution of 3 million electronic medical records, paper cards will not go out of use until the necessary information on the movement and information on the recording of the results of the survey will not be digitized. The task of digitizing maps remains a costly procedure and has not yet been resolved on the scale of distributed territorial medical institutions.

From the above it can be concluded that the digitalization of medical data, the emergence of mobile devices that transmit medical indications, cloud services and artificial intelligence will lead to the solution of the tasks of a “smart” city in the aspect of high-grade and high-quality medical services for the population. This particularly applies to the introduction of telemedicine and medicine, especially in surgery, where robotic systems have already become common.

Thus, the most important objective is to manage the information security of medical data and the use of technologies to protect them not only for one object, but also for the volume of spatially distributed objects connected by telecommunication systems.

Indeed, the leakage of medical information about patients, as information of the highest category in the hierarchy of personal data, is an extremely dangerous and undesirable phenomenon. Threats in this case can be divided into intentional and unintentional [5].

Intentional diversion is a well-organized action to steal medical data for a very specific purpose. They are carried out, as a rule, by employees of the institution and employees of their service companies, for example, firms installing operating systems, updating software, serving databases, and so on.

Unintentional leaks occur from the staff of the institution due to negligence, curiosity, blackmail, as well as misses in the organization of the management system and the protection of information in these medical institutions, violations of access control procedures at the enterprise.

But even more serious threats arise in spatially distributed medical systems that need to interact with each other. They must ensure the openness of interaction and at the same time the integrity of EMR data, the privacy of information about pathologies and health characteristics of the patient's person. This is a very difficult task that is difficult to solve within the framework of existing approaches.

Analysis of medicine and healthcare technologies shows that patient data provided in electronic digital medical records, where all data on the state of human health from the moment of his conception and birth are collected, are primary and most important for creating further technologies. Today, 94% of electronic medical records (EMR) are used in the USA [1]. In 2020 a centralized system will appear in the European Union [4]. Russia is also creating a unified state system. For example, already now in Moscow all state polyclinics of the city are connected to the United Medical Information and Analytical System of Moscow (EMIAS).

The use of cloud technology in telemedicine provides access to patient data for both health care providers and device manufacturers. Information analysis can be carried out remotely, which leads to significant savings.

In Helsinki, a system for identifying and testing the compatibility of drugs based on the analysis of medical records has been developed and implemented.

To ensure the information security of medical data of patients, the integrity of this data, the simultaneous availability of their medical facilities and privacy, it is necessary to develop an effective technology for managing information security and protecting the information contained in electronic medical records (EMR). This technology should provide such a mode of functioning of medical institutions so that the information already recorded in the EMR cannot be falsified, replaced, spoiled and unauthorized authentication of personal data conducted. And also, to exclude the possibility to establish the reception time, the identity of the doctor who entered the data, to identify the laboratory that conducted the patient's analyzes, etc.

Thus, a situation is created requiring the satisfaction of conflicting information requirements set out in an EMR. To date, in our opinion, the above requirements are satisfied by the blockchain technology with cryptographic hashing of data and cryptography methods.

Briton Adam Beck in 1997 invented the mechanism for creating cryptocurrency. For this, the Hashcash anti-spam system was used: the sender performs many time-consuming operations, and the recipient quickly verifies their authenticity.

At the end of October 2008, its technical description and the first version of the code for creating an electronic currency with fully anonymous transactions appeared on the network. Its author was Satoshi Nakamoto. In early 2009, Nakamoto himself created the first wallet. Using the wallet, each of the committed and confirmed transactions is recorded in one of the blocks, which is then attached to the common chain. In 2012 - 2017 the blockchain and hashchain technologies began to develop intensively, not only in banking operations and exchange structures, but also in other sectors of the national economy. In the blockchain, all transactions performed are stored in blocks linked by a special algorithm. It is impossible to change information in a block without being noticed, since changing data will cause changes in the whole block chain. There are users and miners in the system. Users create blocks and internal hashes, and miners build them into a chain and create external inter-block hashes [4,5]. The first advantage of the blockchain is that the base of the blockchain is decentralized, copies are kept by each user, which makes intervention in the database unlikely, as well as the hash functions used in connecting blocks are one-way and crypto-resistant.

The second advantage is the lack of intermediaries. The transaction takes place directly from subscriber A to subscriber B. Miner only provides the service confirming the transaction.

The third advantage is reliability. Blockchain is completely transparent and well protected from data falsification, as it uses digital electronic signature technologies.

The disadvantages include [6], difficulties in scalability, the huge cost of electricity and the constantly increasing weight of the base. Also, the cryptocurrency is still poorly regulated by law, allowing for illegal transactions.

In 2012 - 2017 the blockchain and hashchain technologies began to develop intensively. Despite the fact that the blockchain appeared as a solution in the economic sphere, it has found application in other sectors, including: the organization of private and public administration, authorship and ownership, energy, etc. Further development of the technology blockchain received in the works [7-10].

The success in public administration with the use of blockchain technologies is shown by Estonia, where projects are being implemented in the field of health care. On the basis of the blockchain startup Guardtime, a unified medical base is created that helps to exchange information between hospitals and insurance companies. Prescript in the Netherlands and BitHealth in the USA are working on similar developments.

The introduction of the blockchain in the land cadastre industry solves problems such as fraud, corruption, errors in documents, etc. For example, in Georgia, with the help of BitFury, there already exists a blockchain cadastral accounting system containing more than 200,000 entries. The situation is similar in Sweden with ChromaWay and in Ghana with BitLand. Thus, the solution of the problem of creating elements of the blockchain and hashchain technology theory is very relevant not only for the structures of banking activities, but also for the technologies used in medicine and health care systems and at the same time carrying all the useful properties of the blockchain and hashchain technology. Since there are currently no works that analyze the capabilities of blockchain technologies from a single point of view, from the point of view of their applications in various areas of receiving services, products, goods, the authors took the trouble to develop elements of the theory of blockchain and hashchain technologies. The purpose of the work is to adapt the developed model of network subscribers who are not professional cryptographers and users of computer technologies to fill and process EMR in the field of health and medicine.

Consider the general principles of building systems with a distributed registry, which are based on cryptography methods.

In the most general form, a diagram explaining the operation of N subscribers is shown in figure 1. Here, digital objects are transferred from one subscriber to another with the hash of the second subscriber calculated from the hash of the first subscriber calculated from the hash of the first subscriber, the hash of the third subscriber is calculated taking into account the hash of the second subscriber, etc. A hashchain sequence of blocks connected by a hash function is created. Hash functions that are easy to calculate, but it's impossible to match the input data of a digital object to them, are called cryptographic hash functions. These are the so-called one-way functions: It is easy to calculate x through y, but knowing x it is impossible to calculate y.

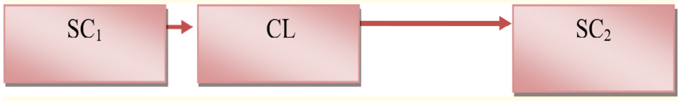

Figure 1: Block diagram of the blockchain technology idea, where SC1 is the computer of the first subscriber, CL is the communication line, SC2 is the computer of the second subscriber.

From figure 2 it follows that the input of the subsequent block generates x φ associated with x φi-1 of the previous block. A possible conclusion follows from this: if you change the data then you must also change the hash function of i-2, i-3... i-N blocks. It is clear that this option is difficult.

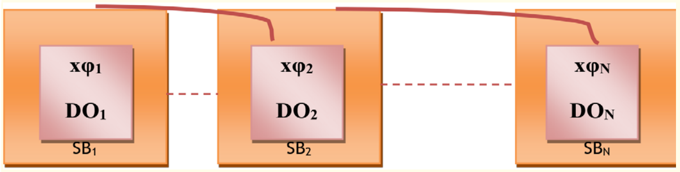

Figure 2: Block diagram of the organization of the hashchain, where xφ1, xφ2 ... xφN - hash functions of the subscriber 1, 2 ... N; SB1, SB2 ... SBN - blocks of subscribers (useful body of the block), DO1, DO2 ... DON - digital objects of the header.

An analysis of these structures shows that, in general, the following characters are necessary members of the set:

1. The subscriber of the network that consumes the service.
2. Subscriber network that provides theservice.
3. The network subscriber who provides the service to the subscriber of the service consumer and the subscriber providing the service for their comfortable functioning in the network and excluding the need to acquire specific skills and abilities by them.

To effectively design networks, it is necessary to create subscriber models that consist of defining information about what the subscriber can do and what the subscriber cannot do. Based on these conditions, it becomes possible to quantify the internal and external parameters, and then shift the subscriber models to algorithms, which in turn allow writing programs in programming languages to implement the blockchain and hashchain network algorithms. The criterion for the belonging of the designed network to the blockchain technology is the mandatory presence of such properties as:

1. Availability of a distributed registry.
2. Decentralization of information processing.
3. The possibility of free control of the reliability of data by any participant (identification and authentication).
4. Practical impossibility of falsification of data of any subscriber of the network and violation of their integrity.

We give a description of the models of the main participants of the network.

1. Subscriber-consumer services (SCS) are an ordinary consumer services.
    a. Skills that SCS owns: knows how to use a computer at a basic level, has a superficial understanding of the operation of the distributed registry system.
    b. Skills that SCS does not own: not a professional in digital technology, does not have knowledge of cryptography, is not able to create the «correct» encryption keys, can not protect itself from hacker attacks.
    c. The SCS must: have encryption keys and EDS received from the certification center, keep private encryption keys in secret, be familiar with the specifics of work in blockchain- related applications and security rules, have a computer (minimal configuration) with Internet access.
2. Subscriber providing services (SPS): is a typical enterprise.
    a. Skills that SPS owns: owns a computer at a level above average, knows the law on personal data, has a good understanding of the work of the distributed registry.

b. Skills that the SPS does not own: it cannot create “correct” encryption keys.

c. The SPS must: have encryption keys and digital signature received from the certification center, keep private encryption keys in secret, be familiar with the specifics of work in blockchain-related applications and security rules, and have a certified information security specialist. Have a working server with personal data protection and Internet access.

d. SPS has the right to: create (using the application) internal blocks and send them to the network, receive internal blocks from other subscribers, verify the authenticity of the author of any internal block in the network, contact Trent to obtain public keys of other network participants or personal for themselves, store and process personal data of SCS.

3. Subscriber-Miner (SM): is a professional notary cryptographer, provides services to other subscribers of the network in terms of the cryptographic design of external units with enabled internal subscriber units.

   a. SM supports blockchain network decentralization. Miner forms the hash function of the external block and includes it in the blockchain and hashchain. The skills that SM owns: professional certified cryptography skills, a full understanding of the blockchain network structure, electrical engineering skills and high-level computer skills.

   b. SM must: have encryption keys and digital signature received from an authentication center, keep private encryption keys in secret, know the full structure of applications and the blockchain network as a whole, have an information security degree, have certified equipment to form external blocks, pass certification before the ability to form external blocks.

   c. SM is prohibited: create internal blocks on its behalf, upgrade the data of internal blocks of other subscribers, receive confidential information contained in the encrypted part of the internal block, delete blocks (both external and internal).

4. The Subscriber Providing Additional Services (SPAS) is a certifying center or Trent: is a government agency responsible for issuing, storing and auditing encryption keys and digital signature.

   a. The skills that ADU possesses are: professional certified cryptography skills, a complete understanding of the structure of blockchain networks, digital skills and high-level computer skills.

   b. The SPAS should: have equipment for generating reliable encryption keys, provide users with encryption keys and digital signature (both their personal and public other network participants), store and protect a database of all subscribers and their corresponding keys.

From the analysis of the described functions, it follows that in any block hashchain network it is necessary to have automated workstations (AWS).

1. AWS subscriber-consumer services: The main conditions of the AWS - the subscriber is not a professional cryptographer and, especially, a cryptographer-cryptographer
2. AWS of a cryptographic notary: The main conditions: the provision of services to subscribers, users and service providers.
3. AWS subscriber service provider: The main requirement is the accuracy of the data provided on payment for services based on regulatory documents and laws governing them.

As an example of a practical application developed by the technology, let us consider the construction of a blockchain network for the EMR corporate network of a medical cluster and its information introduction to other clusters located in a spatially distributed territory.

In figure 3, the algorithm of building a corporate blocket of EMR network is discussed where a new character is involved as a miner: a notary cryptographer. It performs the role of providing the service of embedding the subscribers of their internal blocks with individual hashes using the external block created by them.

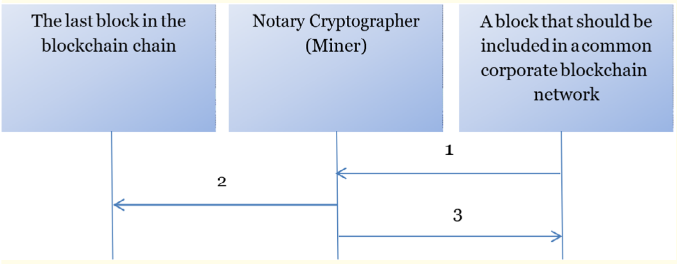
The last block in the blockchain chain
Notary Cryptographer (Miner)
A block that should be included in a common corporate blockchain network
1
2
3

Figure 3: An algorithm for embedding a new unit in the corporate blockchain network of a single medical institution.

1: A block that wants to be included in the general blockchain network provides its notary cryptographer with its IP address and internal hash HBn + 1;

2: The notary-cryptographer receives the external hash of the last block HBn and generates an external hash of the block-enabled HBn + 1 = f (HBn + 1);

3: After the 2nd stage, the notary cryptographer generates an external hash HBn + 1 and gives a command to execute a block that wants to be included in a common blockchain network.

Figure 4 shows the algorithm for creating a new unit in an external network of medical institutions located in spatially distributed territories, but connected by telecommunications information networks. In this case, the internal hash is a common hash of a separate corporate network. The notary cryptographer develops an external hash of the next block and integrates it into a common network.

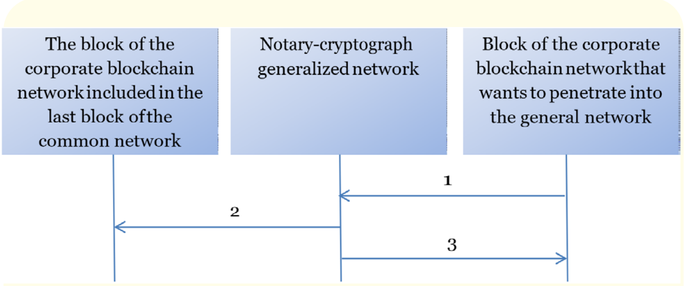
The block of the corporate blockchain network included in the last block of the common network
Notary-cryptograph generalized network
Block of the corporate blockchain network that wants to penetrate into the general network
1
2
3

Figure 4: An algorithm for embedding a new common unit of a medical institution in a common network of blockchains of a spatially distributed network of medical institutions.

1: The block of the corporate blockchain-network xnet will be included in the general blockchain-network, for this it gives its IP address and internal hash HBn + 1;

2: A notary-cryptograph of the generalized network affects the external hash of the last block of the shared network HBn and generates an external hash of the block included in the common network HBn + 1 = f (HBn + 1, HBn);

3: The included block in the total blockchain network.

Discussion

The discussion question of the article is the proposed in the article principle of creating a blockchain network based on the hierarchical method of its structure.

The classical model assumes only a chain structure with a main branch. For discussion, there is a question about the reliable filling of the EMR at the very beginning of its appearance, as well as the question of who will fill the EMR [11-14].

Conclusion

The analysis of the development of medicine and the development of "smart" cities showed that to ensure a compromise condition of accessibility of data provided in electronic medical records, while guaranteeing their integrity and privacy in the interests of the patient, it is necessary to use modern blockchain technology and cryptography. These models of network participants allowed us to develop an algorithm for applying network blockchain technologies based on crypto-resistant hashing for spatially distributed medical facilities related to each other's telecommunication communication networks. Details of the proposed algorithms will be discussed in a separate article.

Bibliography

1. The IBM Watson Health cognitive system - a breakthrough in health care.
2. Digital medicine: healthcare in a smart city.
3. Radiofrequency markings will appear on medical cards in Russia.
4. Association “Fintech” launched the system of accounting for electronic mortgages on the blockchain platform “Masterchain”.
5. Information leaks caused by employees.
6. Robinson A. “What is Blockchain Technology, and What Is Its Potential Impact on the Supply Chain?” (2017)
7. Houy N. “The Bitcoin Mining Game”. *Ledger* 1 (2017): 53-68.
8. Smart E. Top 5 Blockchain Technology Myths the Mainstream Has Fallen For (2017).
9. Gilbert D. Blockchain Technology Could Help Solve $ 75 Billion Counterfeit Drug Problem. Ibtimes (2017).
10. ARMONK Maersk and IBM Unveil Industry-Wide Cross-Border Supply Chain Solution on blockchain (2017).
11. BitFury Group Limited, Prof. of Stake versus Proof of Work, White Paper (2017).
12. Dickson B. Blockchain has the potential to revolutionize the supply chain. Techcrunch (2016).
13. Walch A. “The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk”. *Journal of Legislation and Public Policy* 837 (2015): 851-852.
14. Vorobyev GA., *et al*. “Probabilistic models of cryptographic systems and their applications”. 3rd International Conference on Digital Information Processing, Data Mining, and Wireless Communications (2016): 160-163.

Volume 2 Issue 9 December 2018