A novel architecture of a secure medical system using dag

Shmatko Oleksandr¹
Kliuchka Yaroslav²

¹ PhD, Associate Professor, Associate Professor of SEMIT department; National Technical University «Kharkiv Polytechnic Institute»; Ukraine
² PhD degree student; National Technical University «Kharkiv Polytechnic Institute»; Ukraine

Abstract.
Electronic health information exchange allows providers to healthcare providers and patients to securely access vital medical information of the patient and share it in electronically with other healthcare providers. The paper considers the electronic health system eHealth. The patient's medical records will be stored in a distributed ledger, and not on the server of the medical institution. So no one can change patient data or deny him access to his own data. The use of DAG is considered on the example of the transfer of medical patient data to the doctor. The process of creating and sending medical data to DAG is illustrated with a specific example.

Keywords:
directed acyclic graph
electronic healthcare system
healthcare data exchange
medical patient data
**Introduction** The health sector is undergoing a revolution as technology is embedded in every process. As of today, it is not possible present modern medicine without the use of information communication technologies. Technology can help transform unsustainable health systems to sustainable, establish equal relations between medical workers and patients, provide cheap, fast and more effective solutions to combat diseases [1]. E-health emerged from the need for quality and improved documentation, as well as in tracking the health status of patients and the procedures they undergo. Usually healthcare professionals keep paper records of their patients. However, rising health care costs and technological advances contributed to the development of electronic tracking systems. With development technologies in medicine, a new direction has appeared – telemedicine, in which telecommunications technologies are used to provision of remote medical care [2].

The use of technology has enabled both patients and health professionals to access various resources, which makes health care more efficient and cost-effective. Electronic healthcare provides patients with the opportunity to take active participation in treatment, allowing them to gain a deeper understanding of their condition and ways effective treatment. People are more likely to comply with treatment plans recommended by doctors if they can study the results of the studies of a particular treatment method to learn about the benefits of prescriptions, exercises and other activities aimed at improving their states. This allows patients to clearly understand what exactly their doctor does to help them [3].

The healthcare industry has changed a lot in the last five years. In this is largely due to technology and a large number of innovative digital solutions that are being implemented every day. All these technologies aimed at solving many of the problems that the world is facing medicine [4].

Over the past couple of years, there has been an increased interest in distributed registry technology from the healthcare side, in particular to blockchain technology. Blockchain is one example of a distributed ledger technology. The most important advantage of blockchain is secure exchange
of patient data between medical institutions. However, in recent years, the blockchain has established itself as imperfect technology. Systemic inefficiency and problems scaling led developers to build new networks, which do not use the blockchain data structure at all. For example, IOTA cryptocurrency uses DAG instead of blockchain. If we compare DAG and blockchain, DAG has become more flexible and scalable, and with over time, the digraph becomes faster and more powerful, while the blockchain becomes slower and less productive. In addition, DAG is free, nodes do not need to pay huge commissions for verification transactions. In the blockchain, the transaction fee is too high, or not enough manners to confirm transactions. As a result, nodes need to pay high transaction fees to avoid confirmation delays [5]. Therefore, it is relevant analyze the use of DAG in healthcare to ensure secure data exchange.

**Literature review.** Fragmentation of medical data negatively affects the quality of medical services and patient outcomes. Because health care providers do not have access to up-to-date, complete, timely patient medical data. A patient can visit several medical institutions and each institution will create his own medical card. Since the patient cannot collect all of their medical data together, this can lead to misdiagnosis, duplication of text, selection of the wrong medication, etc. To defragment medical data, the paper [6] proposes to use the Tangle technology, which will facilitate communication between patients and healthcare providers. The use of this technology will improve the quality of medical services and improve patient outcomes.

The work [7] proposes a blockchain-based solution for the exchange of medical data between healthcare providers. This solution ensures the confidentiality, security and availability of medical data.

In [8], a blockchain-based solution for the exchange of medical records is presented. Data is transferred directly between medical institutions. Transparency has improved as the system allows nodes to see and track transactions. The system provides data management, security, and
interoperability. Blockchain technology is a valuable and significant technology for the healthcare system.

BlocHIE is a blockchain platform for the exchange of medical information, presented in [9]. This paper considers two types of medical data: electronic medical records and personal medical data, and also analyzes the various requirements for their storage and exchange. Based on the analysis, the platform uses two loosely-coupled blockchains: EMR-Chain is used for electronic health records, and PHD-Chain for personal health data.

The work [10] presents the Healthchain system for storing medical data based on blockchain technology. This system uses two blockchains (Userchain and Docchain) so that patient data and doctors' diagnoses cannot be deleted or faked. Safety analysis and experimental results have shown that this system can be used in the healthcare sector.

A blockchain-based system for managing and storing electronic medical records is presented in [11]. This system guarantees the transparency and, in particular, the immutability required for safe management and storage, ensuring the efficiency of the system for both clinicians and patients.

**Proposed architecture of secure medical system.** The electronic system of health care eHealth is an information and telecommunication system. This system provides automation of record keeping of medical services and management of medical information by creating, posting, publishing and exchanging information, data and documents in electronic form. It includes a central database (CDB) and electronic health information systems, which provide automatic exchange of information, data and documents through an application programming interface (API).

Software architecture is a program or computing system structure that includes software components, externally visible properties of these components, and relationships between them.

A deployment diagram demonstrates the software architecture. Figure 1 shows the software architecture.
The eHealth system consists of:
- central component (CC) - provides guaranteed availability of information and is responsible for storing and processing information;
- electronic medical information systems - systems that allow you to automate the work of medical institutions from the CDB.

The overall scheme for transferring medical records to the eHealth system is shown in Figure 2.
The main disadvantage of this system is the presence of a single point of failure. That is, if the CC comes out of a standstill, this will lead to the failure of the entire system. The operability of the entire system depends on the CC. Another disadvantage is the lack of a unified medical information system. Since medical institutions can choose any MIS from those that have passed the checks and are connected to the CC of the eHealth system. Also, patients still do not have access to their medical records and cannot get important information at the right time.

Figure 3 shows the transfer of patient medical data to a doctor using Tangle.

![Figure 3](image-url)

**Figure 3**

**Transferring patient medical data to a doctor using Tangle**

A general diagram of the tangle-based medical data transmission system is shown in Figure 4.

First of all, the patient enters the appropriate authorization data. Then the patient searches for a doctor by specialty. From the list obtained, the patient selects a doctor according to the appropriate criteria. After choosing a doctor, the patient makes an appointment for a consultation. In the appropriate window, the patient enters symptoms and complaints bothering him. The patient can get the necessary data from the database (laboratory test results). Based on
this data, transactions are created that are placed in the bundle. The next step is to confirm two unconfirmed transactions. The corresponding request is sent to the node, and we get a hash of the necessary transactions in response. Next, the POW is calculated according to the MWM. Moreover finally, the bundle is broadcast to the network.

![Tangle-based medical data transmission system](image)

**Research results and discussion**

The healthcare industry has faced significant challenges, including interoperability, accessibility, security, and immutability of medical data. Blockchain technology has been used to solve these problems. Because blockchain allows medical data to be stored in a secure, transparent and decentralized manner. Basically, organizations develop their projects in the following areas [12]:

- supervision of the supply chain and the fight against counterfeit products (The MediLedger Project, Ambrosus, Blockpharma);
- telemedicine (PointNurse, Docademic, MDsquare,
TrustedHealth, MyClinic);
- diagnostics (Skychain, DeepRadiology, eHealth First);
- storage and management of medical data (Iryo, Patientory, MedRec, Clinicoin, Medicalchain).

By using blockchain, medical institutions can effectively share medical data while ensuring data privacy and security. Blockchain allows you to track the origin of pharmaceutical products – from the manufacturer to the end consumer. Blockchain also improves telemedicine services by offering remote medical services in a secure, reliable, decentralized, secure and trusted manner.

With the advent of Tangle, organizations have begun to develop medical systems using this technology, and there are already early results. The SmartOptz project allows patients to track their own medical data and share their vital signs with healthcare providers through Tangle. The Pact project provides a secure exchange of medical data between institutions and patients through an API that interacts with Tangle.

This article describes the existing eHealth system in Ukraine eHealth and, as an alternative, proposes a modern approach using Tangle. The presented model will allow healthcare providers and patients to communicate medical data in a secure, transparent and decentralized manner. Tangle can ensure constant data availability through decentralization and lack of a single point of failure. Because the central component of the eHealth system is a central database that accumulates data in a central repository. Failure of the central component will disable the entire system. Blockchain has already proven itself and is used in healthcare systems, as for Tangle, it has a huge opportunity to prove itself in the healthcare industry.

**Conclusions**

Consideration of the mechanisms and features of Tangle leads to the conclusion that this technology is best suited for storing and exchanging medical data. Because when developing healthcare systems, you need to pay special attention to the three main characteristics of Tangle: high scalability, no fees, and instant transactions. High scalability will allow you to process a large/continuous
stream of medical data. The absence of fees allows you to make microtransactions without having to “tip” the miners.

EHealth was considered. This system structurally consists of a central component and medical information systems. The central component is responsible for centralized storage and processing of information and is invisible to end users—patients, doctors. MIS is used for registering patients, making an appointment, maintaining a personal account, issuing referrals, etc. It is these systems that allow end users to cooperate with the eHealth system.

Applications of Tangle are considered on the example of the transfer of medical data of a patient to a doctor. The process of creating and sending medical data to Tangle is considered in detail.

References:


