UDC 004.021

APPLICATION OF BLOCKCHAIN IN ELECTRONIC HEALTHCARE RECORD

Gao Yalu

gr.267011

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus
Tsviatkou Viktar, head of the department of infocommunication technologies

Annotation. Blockchain's decentralized and immutable nature provides a secure and transparent platform for data exchange, guaranteeing data integrity, privacy, and security. This essay endeavors to delve into the potential of blockchain technology in mitigating the issues confronting the healthcare system, with a focus on Electronic Health Record (EHR).

Keywords: BlockChain, Decentralized, Immutable, EHR

Introduction. Given the accumulation of significant personal data[1], it is imperative to establish dependable storage and sharing mechanisms to safeguard patient privacy. Traditional medical data management systems typically rely on centralized servers to construct large-scale site systems or centralized relational database systems, Blockchain, an open distributed ledger based on a peer-to-peer network and consensus algorithm, inherently offers solutions to these issues[2].

Framework Structure of Blockchain. The framework and structure of blockchain can be divided into six layers (figure1): Data layer is where the actual data is stored on the blockchain. It consists of blocks of data that are linked together in a chain. Each block contains a set of transactions, and each transaction contains data that is relevant to the blockchain network. Network layer is responsible for the communication between nodes on the blockchain network. It ensures that data is transmitted securely and efficiently between nodes. The network layer also handles tasks such as peer discovery, routing, and synchronization. Consensus layer is responsible for reaching agreement among nodes on the blockchain network about the validity of transactions and the state of the blockchain[3]. It ensures that all nodes on the network have a consistent view of the blockchain and that no single node can manipulate the blockchain. Contract layer is responsible for providing incentives to nodes on the blockchain network to participate in the network and perform tasks such as validating transactions and maintaining the blockchain. It typically involves the use of cryptocurrencies or tokens as rewards for participating in the network. Application layer is where applications and services are built on top of the blockchain network. It includes user interfaces, APIs, and other tools that allow users to interact

with the blockchain network and access its features.

These layers are intricately interconnected and collaborate to guarantee the security, efficiency, and dependability of the blockchain network. The data layer serves as the bedrock of the blockchain, while the network layer ensures the secure and efficient transmission of data. The consensus layer ensures a uniform perspective of the blockchain across all network nodes, while the incentive layer motivates nodes to engage in network activities. The contract layer facilitates the execution of smart contracts, while the application layer furnishes users with an interface to engage with the blockchain network.

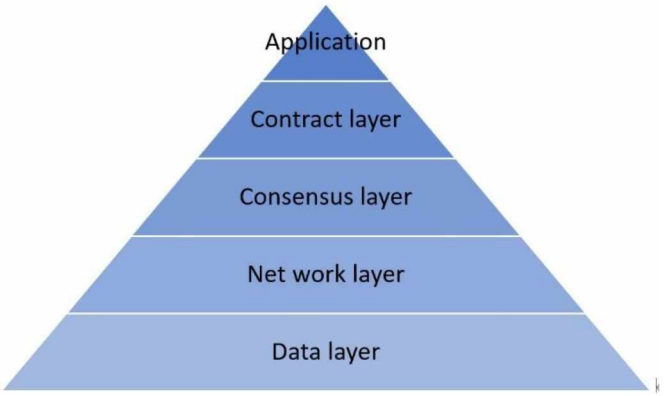

Figure 1 - Structure of Blockchain

Transaction Process. Patient: When a patient visits a hospital, they first register on the hospital server. Upon registration, the hospital server assigns a unique identifier to the patient, equivalent to a medical card. The patient keeps this identifier confidential and presents it during visits. The doctor generates electronic medical records and keywords for the patient, encrypting them using the patient's public key[4]. If the patient seeks treatment at another hospital and the doctor needs access to the patient's medical history, the patient generates a search trapdoor and uploads it to the alliance chain. After running the search algorithm on the alliance chain, the nodes send the encrypted medical records to the patient, who can then decrypt them.

Doctor: Each hospital has a local server and several client devices operated by doctors. When a patient visits, the doctor generates a pseudonym, encrypted electronic medical records, encrypted keywords, and evidence. The doctor uploads the encrypted medical records to the hospital server and the hash value of the medical records, along with the encrypted keywords and evidence, to the private chain. A new transaction is generated and broadcasted. Other nodes on the private chain validate the transaction, and if successful, a new block is added to the private chain.

Data User: When a third-party institution or individual (referred to as a data user) other than the hospital and patient accesses patient data, they require authorization from the patient. The patient generates a search trapdoor and uploads it to the alliance chain. The nodes on the alliance chain perform a search, and when the corresponding patient cipher is found, the nodes act as proxies to generate proxy re-encrypted ciphertexts for the data user. Finally, the data user can decrypt the ciphertext using their private key.

Hospital Server: After the doctor treats the patient and generates electronic medical records, the hospital server extracts the private chain block identifier, patient pseudonym, and keyword index to construct a new transaction on the alliance chain. Other nodes on the alliance chain validate the transaction, and if successful, a new block is added to the alliance chain as shown in Figure 2.

Private Chain: The doctor uploads the hash value of the encrypted medical records and the

keyword index constructed from encrypted keywords and evidence to the private chain, generating a new transaction. Nodes on the private chain validate the transaction. The hospital server extracts the private chain block identifier, patient pseudonym, and keyword index to construct a new transaction on the alliance chain. During the data retrieval phase, if the search is successful, the nodes on the alliance chain extract the secure index from the block to obtain the private chain block identifier. Using the private chain block identifier, the nodes on the alliance chain can retrieve the hash value of the medical record ciphertext.

Alliance Chain: During the search process, when the nodes on the alliance chain receive the trapdoor sent by the patient, they run the search algorithm. If the search is successful, the nodes extract the secure index from the block to obtain the private chain block identifier. Using the private chain block identifier, the nodes on the alliance chain retrieve the hash value of the medical record ciphertext and send it back to the hospital server. The hospital server compares the hash value with the one it has. If they match, the medical record ciphertext is sent to the nodes on the alliance chain, which then return it to the patient. When a third-party data user accesses the patient's electronic medical record, the nodes on the alliance chain act as proxies to generate proxy re-encrypted keys, which are used to perform proxy re-encryption on the ciphertext of the electronic medical record before sending it to the third-party user. System Model Diagram as shown in Figure 2.

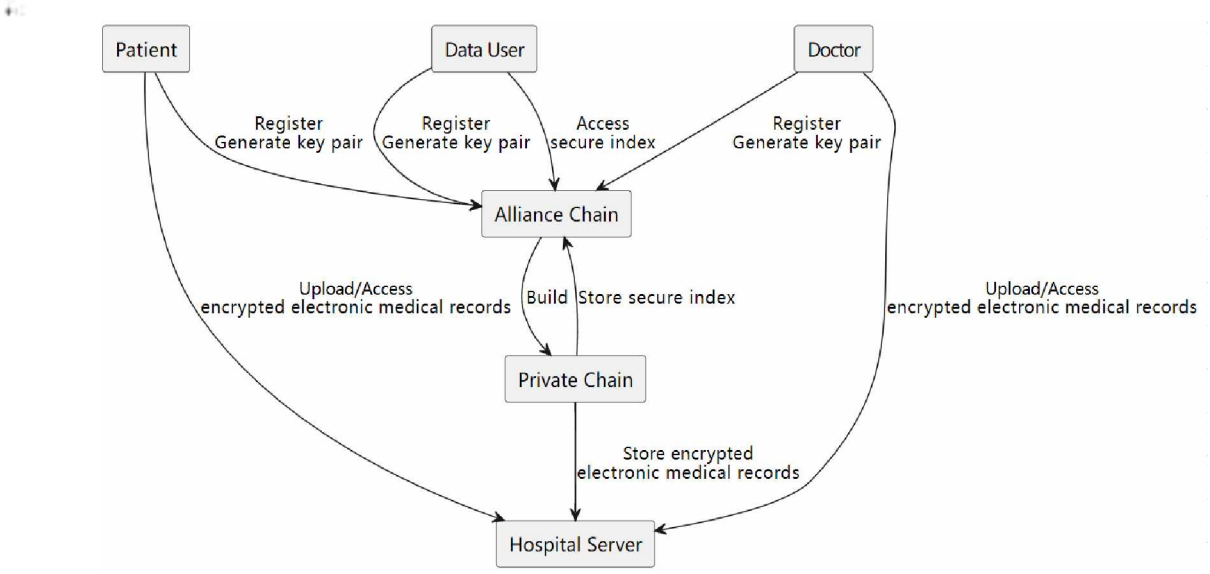

Figure 2 - System Model Diagram

References

1. Hossain, A., Quaresma, R., & Rahman, H. (2019). Investigating factors influencing the physicians' adoption of electronic health record (EHR) in healthcare system of Bangladesh: An empirical study. International Journal of Information Management, 44, 76-87.
2. Menachemi N, Collum T H. Benefits and drawbacks of electronic health record systems[J]. Risk management and healthcare policy, 2011: 47-55.,
3. Quasim M T, Khan M A, Algarni F, et al. Blockchain frameworks[J]. Decentralised Internet of Things: A Blockchain Perspective, 2020: 75-89.
4. Gupta S, Sadoghi M. Blockchain transaction processing[J]. arXiv preprint arXiv:2107.11592, 2021.

UDC 004.021

ПРИМЕНЕНИЕ БЛОКЧЕЙНА В ЭЛЕКТРОННОЙ МЕДИЦИНСКО УЧЕТЕ

Гао ялу

гр.267011

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Цветков Виктор Юрьевич, заведующий кафедрой, профессор кафедры ФИБ

Аннотация. децентрализации и неизменный характер блокчейна обеспечивает безопасную и прозрачную платформу для обмена данными, гарантируя целостность, конфиденциальность и безопасность данных. В этом эссе предпринята попытка углубиться в потенциал технологии блокчейн в смягчении проблем, с которыми сталкивается система здравоохранения, с упором на электронные медицинские записи (EHR).

Ключевые слова: блокчейндецен,трализованный, неизменяемый, EHR