**SỬ DỤNG CÔNG NGHỆ BLOCKCHAIN TRONG HỒ SƠ Y TẾ ĐIỆN TỬ**

***Nhóm: Vũ Quỳnh Anh - 2001040010,***

***Lê Hồng Ngọc - 2001040152,***

***Ngô Thị Quỳnh - 2001040180,***

***Đặng Quỳnh Trang - 2001040208***

***Đơn vị công tác: Đại học Hà Nội***

***Giáo viên hướng dẫn: Đặng Đình Quân***

*Công nghệ blockchain từ lâu đã được xem là một đề tài nghiên cứu hấp dẫn, và nhiều doanh nghiệp khác nhau đã tận dụng lợi thế của nó. Tương tự như các ngành công nghiệp khác, ngành y tế cũng có rất nhiều lợi ích từ công nghệ blockchain do tính bảo mật, riêng tư, bảo mật và phi tập trung của nó. Tuy nhiên, trong các hệ thống Hồ sơ Bệnh án Điện tử (EMR), vẫn tồn tại vấn đề về bảo mật dữ liệu, tính toàn vẹn và quản lý. Trong nghiên cứu này, chúng tôi mô tả cách áp dụng công nghệ blockchain để thay đổi các hệ thống EMR và tiềm năng giải quyết những vấn đề này. Chúng tôi cung cấp một khung nhìn có thể áp dụng cho việc áp dụng công nghệ blockchain cho hồ sơ y tế điện tử trong ngành y tế. Mục đích của khung nhìn được đề xuất của chúng tôi là áp dụng công nghệ blockchain vào EMR và thông qua việc thiết lập điều khiển truy cập tinh thể cho người dùng của khung nhìn được đề xuất, cung cấp lưu trữ an toàn cho các bản ghi điện tử. Ngoài ra, bằng cách sử dụng lưu trữ bản ghi ngoài chuỗi, phương pháp này khám phá vấn đề về tính mở rộng của công nghệ blockchain nói chung. Một giải pháp tích hợp, bảo mật và mở rộng dựa trên blockchain được cung cấp cho hệ thống EHR nhờ kiến ​​trúc này.*

**USING BLOCKCHAIN TECHNOLOGY IN ELECTRONIC MEDICAL RECORDS**

*Blockchain technology has long been a fascinating research topic, and many different businesses have taken use of its advantages. Similar to other industries, the healthcare sector has a lot to gain from blockchain technology because of its security, privacy, secrecy, and decentralization. However, there are issues with data security, integrity, and management in the Electronic Medical Record (EMR) systems. In this study, we describe how blockchain technology can be applied to change the EMR systems and potentially provide a resolution to these problems. We provide a framework that might be applied to the adoption of blockchain technology for electronic health records in the healthcare industry. The purpose of our proposed framework above is to apply blockchain technology to EMR and by establishing granular access controls for users of the proposed framework, to provide Secure storage of electronic records. Additionally, by using off-chain record storage, this approach explores the scalability issue with blockchain technology in general. A scalable, secure, and integrative blockchain-based solution is made available to the EMR system thanks to this architecture.*

# 1. Introduction

The rapid evolution of technology is progressively exerting its influence on all facets of human existence. The advancements in technology bring substantial benefits to the healthcare industry, including enhanced security, improved user experiences, and other aspects. The implementation of Electronic Health Record (EHR) and Electronic Medical Record (EMR) systems has yielded substantial advantages. Although these systems offer numerous advantages, they encounter various challenges associated with the veracity of data, safeguarding of medical records, as well as the ownership of data by users. Blockchain technology represents a novel solution to address this issue. The blockchain technology offers a secure, impregnable, tamper-resistant, and deception-proof medium for preserving medical records and other healthcare-related data. Preceding the emergence of modern technology, the healthcare profession or medical enterprise relied on a manual mechanism through which medical records were stored on paper and documented using handwritten means. The manual system encountered various issues, including duplication, data redundancy or errors, attributable to the presence of multiple copies of the patient's medical records across the facilities that they visited. The objective of implementing EMR systems is to address the challenges encountered with paper-based medical records and establish an efficient technological infrastructure capable of revolutionizing the healthcare sector. The implementation of EMR systems across several global hospitals has been undertaken to augment security and cost-effectiveness while availing themselves of the numerous benefits these systems offer. Blockchain technology offers a promising solution that not only solves the protection and circulation of medical records, but also ensures the privacy of patient personal information by legally transferring data ownership. This research paper is organized into two sections: section II is a basic summary of blockchain technology and section III is an explanation of the design, architecture, and performance of using blockchain technology in electronic medical records. Our code is published on “https://github.com/belemon81/UsingBlockchainForElectronicMedicalRecords” as a reference.

# 2. Overview of blockchain technology

Blockchain is a platform for storing transactional data using linked blocks that undergo constant expansion. It uses a decentralized methodology, which enables shared ownership of each data element and facilitates the dispersion of information. The platform also utilizes hash functions to provide a layer of security to the processed data, offering enhanced security, anonymity, and data integrity without the need for third-party mediation. Due to its advantages, blockchain is an ideal choice for retaining sensitive information such as patient medical records.

Blockchain's three main features are decentralization, data transparency, and security and privacy. Decentralization allows information to be disseminated across a network, facilitating control based on consensus achieved through shared input. Data transparency requires cultivating trust and ensuring security and integrity, with data dispersed throughout the network to prevent unauthorized tampering. Finally, security and privacy are ensured through cryptographic functions, with the SHA-256 algorithm used to generate hash values that maintain data integrity and prevent extraction. The decentralized nature and robust cryptography of blockchain make it a viable choice for safeguarding privacy in certain applications.

# 3. Applying blockchain technology for electronic medical records

## 3.1. The principle of sending and receiving electronic medical records in P2P network

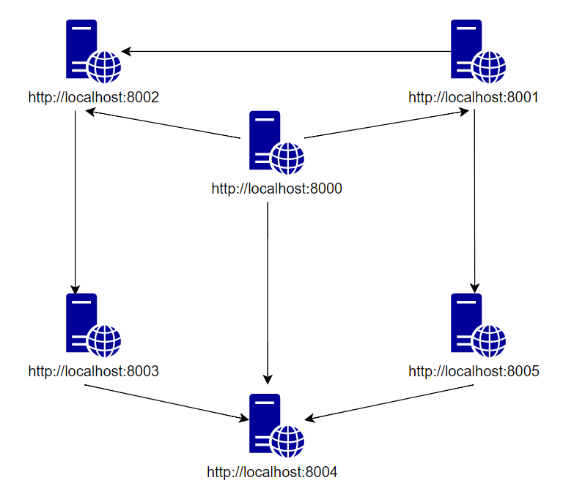
Blockchain technology has the potential to revolutionize the healthcare industry through secure and efficient exchange of medical records. Each node maintains a copy of the blockchain, which acts as a decentralized ledger that records all EMRs, resulting in faster diagnosis and treatment times. This technology enhances the security of medical data by utilizing cryptographic algorithms and distributed ledgers to protect against unauthorized access and tampering. Additionally, the decentralized nature of the blockchain ledger eliminates the need for a central authority to manage and maintain medical records, making it more efficient and cost-effective.

In the decentralized network used in our development, EMRs are broadcasted and verified by nodes before being added to the mempool. Once confirmed by a miner and added to the blockchain, the medical records become permanent and accessible to all nodes. Queries can be made to retrieve necessary information, allowing for secure and efficient medical record transfers without the need for a centralized intermediary.

### 3.1.1. Architecture

The principle of sending and receiving medical records between nodes involves the transfer of medical data between healthcare providers, such as hospitals, patients’ family members, patients, doctors, nurses, miners, and other relevant people.

In our simulated P2P network, Miner8000, Miner8001, Node8002, Node8003, Node8004, and Node8005 represent the programs run in each node. They are connected to each other, making it possible to transmit data between nodes; any updates can be synchronized across the network.



Our network consists of various nodes represented by different programs using Node, each with unique port numbers. One such program provides APIs using Flask() and @app.route().

Otherwise, based on our development on the topic of Applying Blockchain for Electronic Medical Records, we included the class MedicalRecord, which contains some of the essential information required for the creation and maintenance of medical records, such as Hospital, Patient and Diagnosis. The class will later be used to reflect a complete EMRs and validate its information before being sent to another node in the P2P network.

In summary, the use of classes helps define the essential information required for creating and maintaining medical records, and interconnected nodes ensure that data can be transmitted and updated across the network.

### 3.1.2. Implementation

In the code provided, the Node class represents a node in the blockchain network. Each node has a unique identifier (ID), its keypair including public key and a private key, and a list of peers (peers) to which it can communicate.

#### 3.1.2.1. Sending medical record from a node to other peers in the network

In Node functions, send\_medical\_record() is responsible for creating and sending a medical record to other nodes. Receiving the receiver's ID, medical record data and a fee as input, it creates and verifies the medical record using create\_medical\_record() and verify\_medical\_record() functions. If successful, the medical record will be added to the node's mempool by add\_to\_mempool() and broadcasted to the other nodes using forward\_medical\_record(). A confirmation response is sent back to the sender to confirm the broadcast.

To be more specific, create\_medical\_record() helps to create a JSON object that contains the medical record, time, sender, receiver, and fee, which will then be hashed and encoded using SHA256 and RSA algorithms to provide a unique “digital signature”. The function will return the packet with some other important keys: “type” to validate the medical record, “age” to keep the medical record sent in finite times, and “tracking” and “forwarder” to prevent the medical records from being sent to a node the second time. Afterwards, verify\_medical\_record() function helps to check whether the hash gained from decoding the digital signature using the public key of the node is equivalent to the hash of the data. If the verification is successful, the add\_to\_mempool() function adds the medical record to the node's mempool while preventing duplicates. The mempool ensures the security and privacy of medical records by restricting access to authorized parties only, even if unauthorized parties gain access to the blockchain.

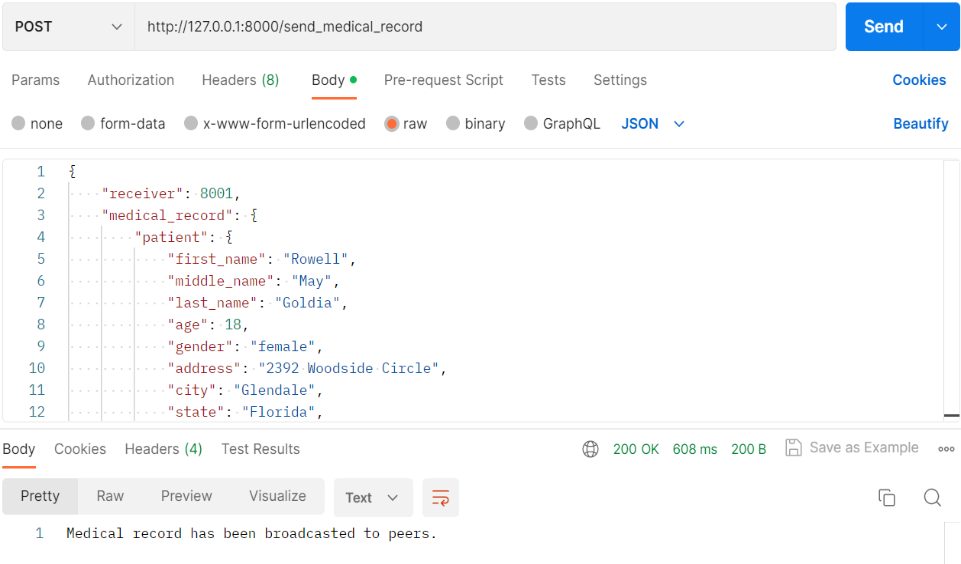
The forward\_medical\_record() function helps to forward medical records to other network nodes. It creates a new thread to send the record to each peer asynchronously, except for the original forwarder and the sent nodes. The node stops forwarding when the "age" is zero.

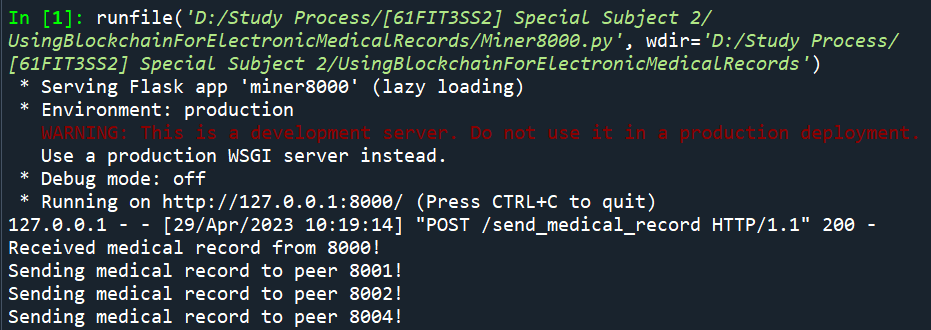
#### 3.1.2.2. Sending medical record from a node to other peers in the network

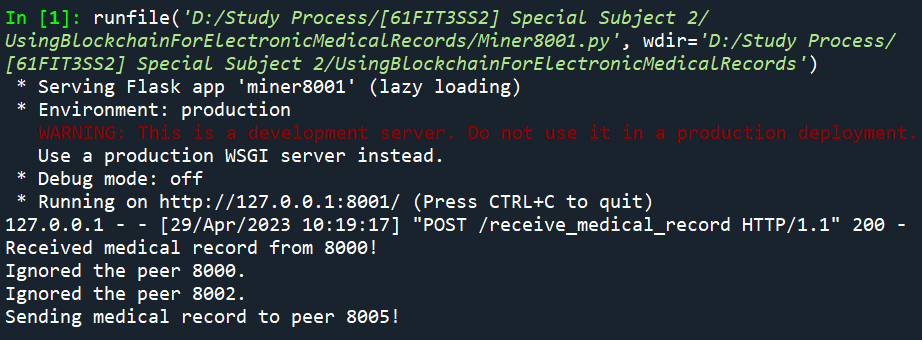
On the other hand, when a node receives a medical record from another node, the receive\_medical\_record() function is called to validate its digital signature and determine whether it should be added to the node's mempool. The function checks the data object's type and verifies the medical record's validity using the verify\_medical\_record() function. If the verification succeeds, the medical record is added to the node's mempool and broadcasted to other nodes using the forward\_medical\_record() method.

### 3.1.3. Demo for the principle of sending and receiving electronic medical records in P2P network.

By using Postman and Firefox applications, we intend to demonstrate the result of sending and receiving medical records from other nodes in our experimental network. By sending a POST request containing the medical record from Miner8000 to its peers, we got the response below, which denotes that the medical record was sent successfully.



As shown in the network diagram provided, Miner8000 is responsible for sending information  to peers Miner8001, Node8002 and Node8004. Thus, some logging messages from the console.

Here we showed an example demonstrating how Miner8001 had successfully received medical records from peers. After sending medical records to peers, the senders (or forwarders) would ignore if their peers forward the medical records back.

Afterward, to view the result of the medical record, we browsed “http://localhost:8001/recent\_medical\_record”. Consequently, we got the medical record “packet” composed of the EMR data, the public key, and the digital signature.

In conclusion, the principle of sending and receiving medical records in a blockchain-based healthcare system is based on encryption and digital signatures for data integrity and authenticity. A decentralized ledger and mempool enable efficient and reliable node communication, while age limits prevent spamming and sustain the network. The experimental source code provides a basic implementation, but more research and development are required to fully utilize blockchain in healthcare.

## 3.2. The principle of using blockchain to store electronic medical records

By increasing the accuracy, security, and accessibility of medical records, blockchain technology has the potential to revolutionize the healthcare business. However, adding medical records to the blockchain is a complex process that involves the use of mining blocks and mempool. Mining block refers to the process of adding new data to the blockchain by solving complex mathematical puzzles using computer power, creating a permanent and unalterable record of data. This ensures the patient's information is secure, private, and cannot be tampered with. The mempool also plays a crucial role in saving medical records to the blockchain, ensuring that they are not lost or duplicated (Nakamoto, 2008).

The receive\_block() method in the Node program is called when a node receives a new block. It first checks whether the block is valid by calling is\_chain\_valid() and is\_block\_valid() from the blockchain attribute which is an instance of the Blockchain class. If the block is valid, it checks whether each medical record in the block is valid by calling verify\_medical\_record(), and if any record is invalid, the function returns an error message. Otherwise, the method appends the block to the blockchain and sets a flag to indicate that a new block has been received. It then forwards the block message to all other peers in the network by calling the forward\_block() method.

Specifically, the is\_chain\_valid() function checks the validity of the entire blockchain by iterating through each block and verifying its hash and previous hash. It starts by checking the last block's hash and then checks each block's hash and previous hash while iterating backwards. Meanwhile, the is\_block\_valid() method checks if an individual block is valid by verifying the index, previous hash, and hash satisfaction of the target hash.

The hash() method plays a crucial role in hashing a block by converting it to a JSON string, encoding the string, computing the SHA256 hash, and returning the hexadecimal representation of the hash. The satisfy\_target() method checks if a hash meets a specified target. The target in this case is to have the hash start with four zeros, which makes mining a new block easier for the mine.

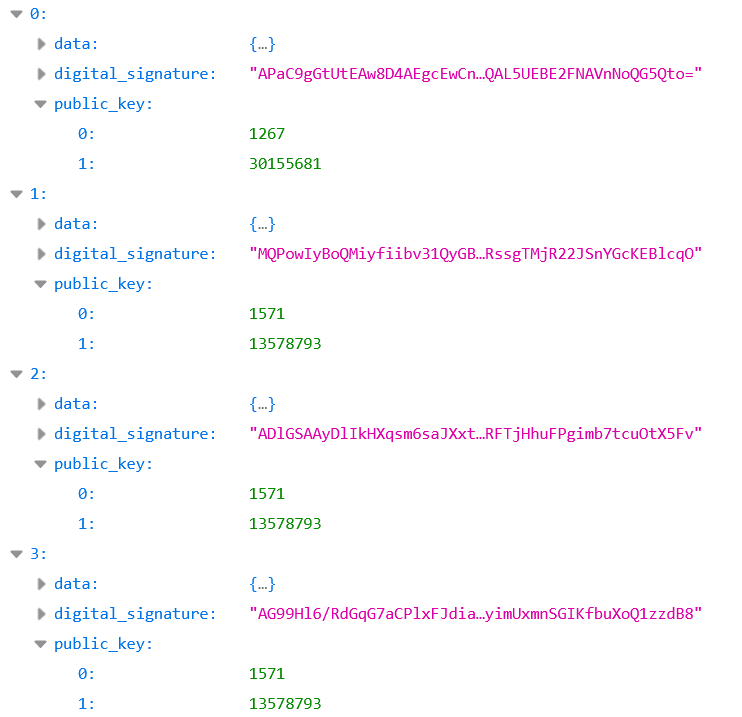
The forward\_block() function in the Node class is called when a block is received and needs to be forwarded to other nodes in the network. This method checks the block's age and decreases it if it's greater than 0. It then sends the block to peer nodes that haven't received it and adds the current node's ID to the block's tracking list. The method is similar to forward\_medical\_record().

Pivotally, before a medical record can be added to the blockchain, it must first be stored in the memory pool. According to Antonopoulos (2015), the mempool serves as a temporary storage for unconfirmed transactions, which includes encrypted medical records in our project. These records remain in the mempool until a miner confirms and adds them to the blockchain. In our codebase, the Miner class is responsible for implementing the mine block principle and the use of the memory pool.

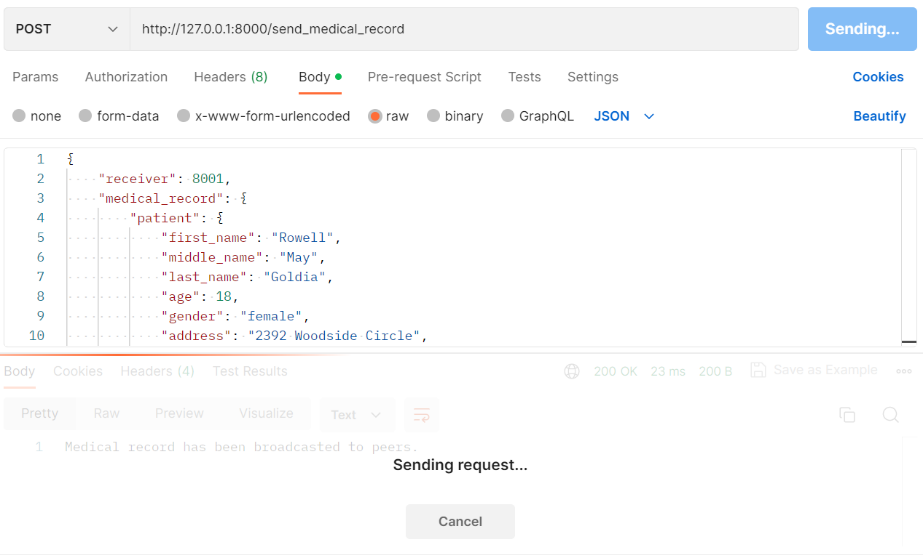
The add\_to\_mempool() function of the Miner class is used to add a new medical record to the memory pool. This function overrides the method of the parent class with a minor modification, that is, if the total size of the mempool plus the size of the new record is more than 500 bytes or the total number of the medical records in mempool exceeds 10, the Miner will mine the block. The Miner class uses the mine() function to create a new block and add it to the blockchain. It performs proof-of-work by repeatedly generating a hash and incrementing the nonce until a valid hash (starting with four zeros) is found. Once complete, the block is added to the chain, the mempool is cleared, and the new block is broadcast to other nodes. The process prevents spamming and denial-of-service attacks. A fascinating point in the mine() method is that each of the Node includes an attribute called “new\_block\_triggered”. This attribute actually has no impact on a not-a-miner Node, but to a Miner, it can help to stop the mining process when a new block comes as a valid block. To minimize time and efforts spent to mine the next block, the Miner will stop the current mining process to achieve the new block to the blockchain and find another opportunity to be the winner next time. Finally, the send\_block() function is called by the mine() function to broadcast the newly mined block to other nodes in the network, checking the type of the message received, and forwarding it to the other nodes if the block is valid.

Overall, these functions work together to maintain the integrity of the medical record system by ensuring that only valid and confirmed medical records are added to the blockchain.

To monitor the flow of the mining process referred to in this paper, we continue to use the same testing data of section 3.1. The medical record is visually duplicated, but the timestamp makes it different each time it is sent to another peer. Firstly, may we desire to view all the pending medical records in the mempool of one node. Therefore, a GET request was sent to the URL “http://localhost:8000/pending\_medical\_records”, helping us view the fair result.



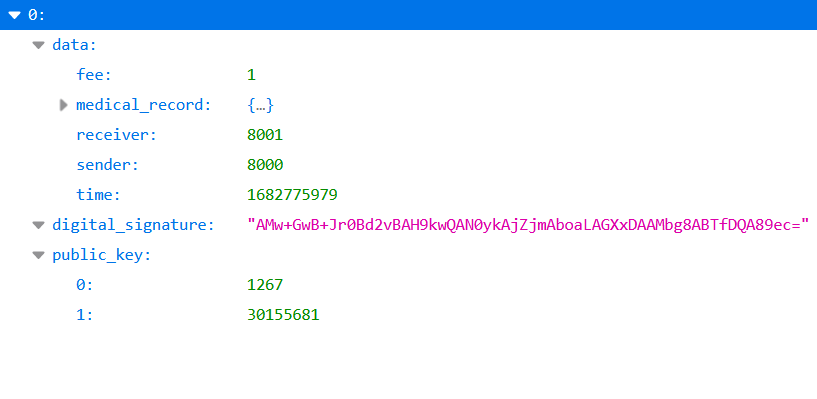
Second, recall that the mining process would automatically start when the mempool of a node reaches block’s capacity (500 bytes) or at most 10 medical records (the condition is to reduce the tension of pending medical records). Accordingly, we kept sending the medical records to the receiver, until the screen stuck at the sending screen.



This is the typical sign that the current node was in the mining process. Waiting until the end, we can check the node’s blockchain by viewing “<http://localhost:8000/verified_medical_records>”



Finally, checking one of the nodes’ mempool will result in a refreshed result.



In summary, the mine block principle and use of mempool are crucial for ensuring the integrity, security, and accessibility of medical records on the blockchain. Mempool enables quick and secure processing of medical records, providing medical professionals with timely access to patient information. As the healthcare sector adopts blockchain technology, the significance of mempool in enhancing blockchain-based healthcare systems will only increase.

# 4. Conclusion

This paper elucidates the healthcare advantages of blockchain technology and its potential application in facilitating Electronic Medical Records. Despite the considerable progress made in healthcare and the technological advancements seen in EMR systems, unresolved issues remain with regard to blockchain technology implementation. The proposed framework comprises a secure record storage system coupled with a comprehensive set of access regulations governing the management of said records. This phenomenon yields an operational framework that is characterized by enhanced user-friendliness and comprehension, particularly with regard to user-system interactions. The implementation of user role-based access in a system confers numerous advantages, including increased security and privacy for medical records. Specifically, such access controls limit access to trusted and relevant personnel exclusively. Furthermore, this approach effectively addresses the issue of information asymmetry plaguing the EMR system. In light of this, our future research plan includes three issues: finding a way to fashionably display on the website the information of a particular medical record, the blockchain or the mining process; adjusting mining difficulty in accordance with the growth of the blockchain; and dealing with the changes of EMRs even after saving to the blockchain.

# REFERENCES

1. Antonopoulos, A. M. (2015). Mastering Bitcoin: Unlocking Digital Cryptocurrencies.

2. Borade, S., Paradkar, T., Takalkar, P., & Trivedi, A. (2023). Blockchain Based Electronic Health Record Management System. Retrieved from https://ssrn.com/abstract=4376765

3. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf