COMP3050 Individual Dissertation Single Honours

Dissertation

Medial Blockchain for Smart Health Home

Submitted April 25th, 2022, in partial fulfilment of

the conditions for the award of the degree BSc Computer Science.

Haonan Chen (20124862)

Scyhc3@nottingham.edu.cn

Supervised by Prof. Vladimir Brusic

School of Computer Science

University of Nottingham Ningbo China

I hereby declare that this dissertation is all my own work, except as indicated in the text. Date: 2022/04/25

Acknowledgement

I would like to express humble gratitude to my professors, supervisors, Prof. Vladimir Brusic, who assisted me to complete the project, for all the motivation, supervision, guidance, and encouragement throughout my project.

I would like to thank:

Dr. Tianhong Cai, Dr. Xiang Zhang, Dr. Yinglun Li and all the PhD students in smart health home group, for all the assistance, experience sharing, and encouragement throughout the project.

Prof. Matthew Pike, for all the help, assistance, and encouragement throughout the project.

Mr. Xiaochen Zhao, Mr.Yichun Jiang, Mrs. Wenhui Tu and all the colleagues in wanxiang blockchain company, for guidance and experience sharing in the field of blockchain during the 2021 summer internship.

My family, for their continued support to my study and life.

Abstract

We designed and implemented a medical blockchain system for the Smart Health Home environment. This Medical Blockchain is a part of medical data management with the main purpose to enable safe and secure data sharing between patients, specialized data exchange centers, and hospitals. We designed the protocol for data exchange between edge computer, data exchange center, and hospital computer. This system is a part of the smart medicine project from the Smart Health Home project. The system collects data from wearable sensors, processes them and transfers the reports to medical practitioners. The system must ensure efficient, safe, and secure data transmissions between the nodes, therefore medical blockchain is a critical part of the overall system. Our medical blockchain uses the Hyperledger Fabric (an open-source blockchain platform from the IBM Company) as the kernel blockchain framework. In our medical blockchain system, patients and hospitals are members of the alliance chain and have their nodes as blockchain nodes. Doctors can send the requirement for data to their patients and patients can upload corresponding data from edge computers to the data exchange center. Medical doctors can access the uploaded reports from the exchange center. The main goal of this medical blockchain system is to provide a trusted environment between Smart Health Home and the hospital for improved health care delivery.

Content

List of Tables and Figures

Figures

Tables

Terms and Concepts

1. **Blockchain:** A blockchain is a growing list of records, called blocks, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and a transaction.
2. **Smart health home (SHH):** A concept of the home environment which contains IoT devices, mobile devices and edge computers for healthcare and health monitoring.
3. **Data exchange center (DEC):** A big database that allows users to upload the health report and doctor could use his authentication and report address to get the data.
4. **Smart Contract:** A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and agreements exist across a distributed, decentralized blockchain network.
5. **Hash Value:** A hash value is a harmless looking string of hexadecimal values, generally 32 to 64 characters long, depending on the hash algorithm used. There is absolutely nothing in a hash value that will tell you anything about what was hashed or how big it was.
6. **Public/Private key:** The public key is used to encrypt, and a private key is used decrypt the data. The private key is shared between the sender and receiver of the encrypted sensitive information. The private key is used to both encrypt and decrypt the data. This key is shared between the sender and receiver of the encrypted sensitive information. The private key is also called symmetric being common for both parties. Private key cryptography is faster than public-key cryptography mechanism.
7. **Health Report:** A report includes the specific type of medical data measurement results and follows given protocols

1 Introduction

The advances in IoT technologies enable the creation of a Smart Health Home environment, which enables the collection, processing, and transmission of health and related data in real-time. Combining medical-grade wearable devices with wearable sensors and mobile applications enables, a personal medical report can be generated and used to catch vital signals when emergencies come when going to hospitals is not in time. The medical data storage and transmission regulations require strict protection of identities and data integrity. A blockchain-based platform is necessary to plug into the Smart Health Home system to solve the privacy problems and establish a trusted environment for data sharing and transmission. This section describes the background and motivation of this project and provides the aims and objectives of the project.

1.1 Background and Motivation

1.1.1 Foundations

Smart Home

The smart home concept initially came up as a cost-effective and promising solution to improve the quality of living at home for elderly and disabled individuals [1]. The proposed solution included improving comfort, helping with medical rehabilitation, and health monitoring (movement, vital signs, health condition). The growing number of IoT devices shapes the functionality of the Smart Health Home environment by providing for the real-time collection and analysis of health-related data. Smart home environments contain sensors, medical devices, and other IoT devices for data collection. Usually, data processing and storage are done within remote data centers [1].

Blockchain Technology

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network [2]. The ledger is a linear linked list of blocks arranged in chronological order, in which information about transactions is stored and can be seen as a distributed database technology that enables the transfer of value over the network with a foundation of trust. Bitcoin [3] was introduced and blockchain technology, the technical framework underlying Bitcoin, began to enter the limelight. Due to the decentralized nature of blockchain, it not only supports scalable applications such as automatically executed smart contracts but also focuses on key technologies such as data security and privacy protection, which

makes blockchain technology successfully applied in the field of digital cryptocurrency and a wide range of some application scenarios in economic finance, IoT supply chain and social public services. In the medical field, Blockchain technology was proposed for managing smart home data [4], managing health data [5], medical data sharing [6], and management of the Internet of Medical Things (IoMT) [7].

1.1.2 Current Trends

The era of Big Data is characterized by high volume, the velocity of acquisition, variety and variability of data types, requirement for accuracy and trustworthiness (veracity); the analysis of data is expected to create value, and it is usually communicated to the user by visualization techniques [8]. Wearable Sensor Networks (WSNs) provide massive real-time data streams, presenting new challenges as compared to the traditional data management systems [9]. In the health care field, particularly home health care, sensors such as accelerometers, heart rate monitors, breathing sensors, sleep monitors, or medical devices such as ECG, blood pressure or blood glucose meters, and thermometers are increasingly used for continuous or protocol-based monitoring such as rehabilitation and health monitoring [10]. With the availability of medical-grade wearable devices and emerging mobile applications, the personal medical report enables real-time to capture vital signals and other relevant data, provide alerts, and generate reports when needed. Because medical data require the highest level of data safety and security protection, the storage and transmission of health data require strict protection of privacy and the highest level of data integrity.

1.2 Motivation

Smart Health Home (SHH) is an emerging environment that provides continuous health monitoring services using IoT devices, and mobile health applications. It enables continuous collection of data and, together with edge computing applications, real-time analyses, and transfer healthcare providers [5]. To solve the privacy and safety problems and establish a trusted environment for data sharing and transmission, blockchain technology is proposed as the solution to the SHH system. Blockchain technology is considered a system that offers high data security because data encryption is an essential part of blockchain systems. Nevertheless, some vulnerabilities of blockchain systems, such as hard to maintain, and high cost of technique learning are known [11].

Sensor systems, particularly those used in medical applications collect large amounts of health data that need to be matched with personal information to provide health care. Telemedicine and home health care often require data transfer and information processing in real-time creating a need for safe and secure data sharing. Blockchain enables a convenient way of protecting data integrity and easy sharing [12]. Medical blockchain has been considered for [5]:

1. Mitigation of errors resulting from data collection and interpretation
2. Improvement of medical outcomes in telemedicine, eHealth (electronic health), home health care, and mHealth (mobile health)
3. Ensure traceability of medical reports

Many research and analysis are based on a great amount of well-organized and validate data. If such a system allows users to share anonymous data and medical institutions to use it, it will be convenient and helpful. The main reasons why we need to build such a medical blockchain system include the requirements of security, and accuracy of data transfer [6]. These criteria require the health data validated (data are accurate and calibrated), verified (from a person in SHH), and safely transmitted. Additional benefits include establishing standardized channels of communication between patients and hospitals that must be both efficient and timely. Medical data transfer can be combined with a payment system that enables payments for medical services and keeping legally valid records.

1.3 Aims and Objectives

In this project, we propose the development and implementation of a health blockchain for the management of personal health data generated by SHH used in health care**.** The overall structure of the proposed system is shown in Figure 1.

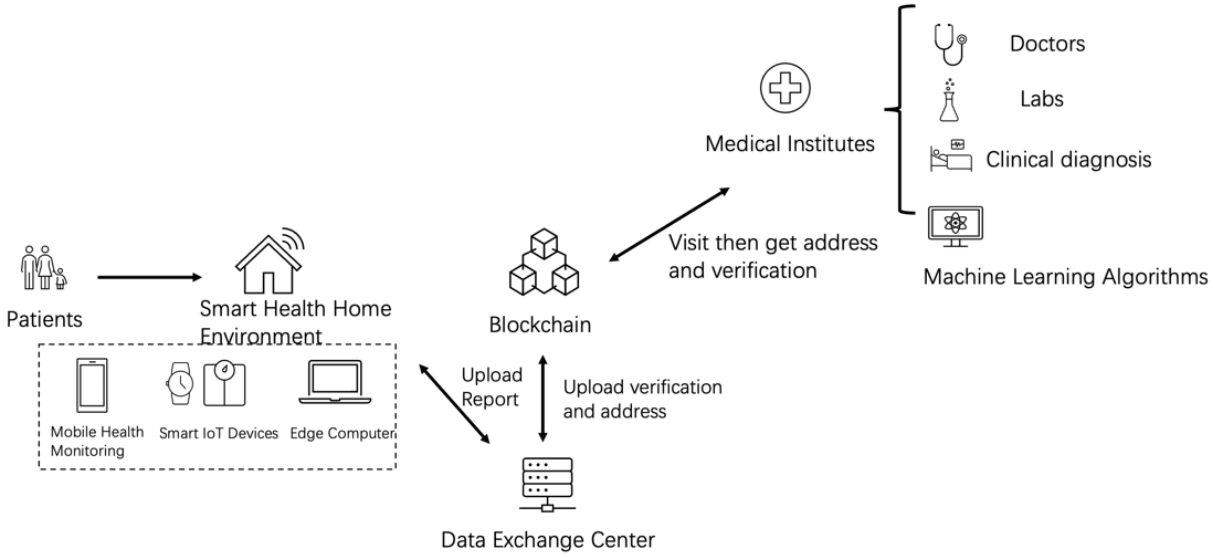


Figure 1: The overall structure of home health care system with embedded Medical Blockchain

We design, implement, and test a blockchain-based SHH system for medical data management and sharing between nodes: Smart Health Home, data exchange center, and health care institution. The main goal is to ensure efficient, safe, and secure data transmissions between the nodes. The blockchain system controls the transmission of identifiers that protect the ownership of personal health data and permission certificates for access the personal health data. Authorized medical institutes need secure and timely access to anonymized data featuring safe and secure identification. The main requirement of this system is to make its operation error-free and timely.

The **specific objectives** of this project are:

1. Design the medical blockchain system and interaction interface with Smart Health Home.
2. Design and simulate the Data Exchange Center to interact with smart homes and doctors in medical institutions.
3. Design a pattern for Authentication verification between patients and doctors to control the scope of access in the blockchain system and data source.
4. Design several protocols of medical data reporting, for different types of measurements as the study cases.
5. Develop an appropriate encryption procedure for data transmission
6. Implement a solution to receive a report from the data exchange center and upload ledger data to the blockchain.
7. Develop a smart contract of blockchain to allow upload and query of the information on the blockchain.
8. Develop the front-end and back-end to enable user interactions and activities including data updating, data downloading, requesting data sharing, confirming a request, and transferring reports.
9. Plug in the credit system in the original system to allow users to gain credits for data open sourcing.
10. Write and publish a conference article (desired).
11. Complete on time the dissertation and other required deliverables.

1.4 Dissertation Outline*

This thesis consists of seven sections, a Bibliography, and an Appendix. The sections are Introduction, introduces the background, goals and objectives of project; Related Work, literature review about techniques used in this project and existing applications of blockchain for medical usages; Methodology, the methods I used during this project (research and software engineering); Design, the design of whole system and each component; Implementation, the technical implementation of medical blockchain system; Summary, the project conclusion and future work; Evaluation, reflection of whole project and project management.

2 Related Work

This section includes a literature review in the field of blockchain technology and applications in the storage system and medical purposes. This section also introduces some basic concepts from relevant papers and analyze existing systems that are partially like our proposed medical blockchain system.

2.1 Blockchain Technology

Bitcoin [3] is one of the most successful blockchain applications. With its successful adoption and wide dissemination, the underlying technical principles are attempting to demonstrate greater value. Blockchain technology has three significant features: blockchains are decentralized, immutable, and traceable [14].

2.1.1 Decentralization

The underlying technology of blockchain is a peer-to-peer (P2P) computer network. The network participants' qualifications are fully reciprocal [15]. The blockchain allows for the peer-to-peer transfer of value because the of P2P protocol. And this feature provides a freer, more transparent, and fairer environment that gives individuals more choice and opportunity.

2.1.2 Immutability

A blockchain can be thought of as a distributed ledger, where each page of the ledger is a block. Each block stores all the changes in state and the results of transactions in a certain period of the network, and the blocks are linked together to form a chain-like structure [16]. In a blockchain, the first block is called the genesis block and usually contains no transaction information. The genesis block determines the block structure. The block consists of a block header and a block body. The block header contains the block number, the current block hash value, the previous block hash value, a timestamp, and other public information. Each block contains the hash value of the previous block, linked to the first and last block by a hash pointer. Newly generated blocks are timestamped and can only be appended to the end of the main chain, forming the longest legal chain (ledger) from the creation block to the current block [15].

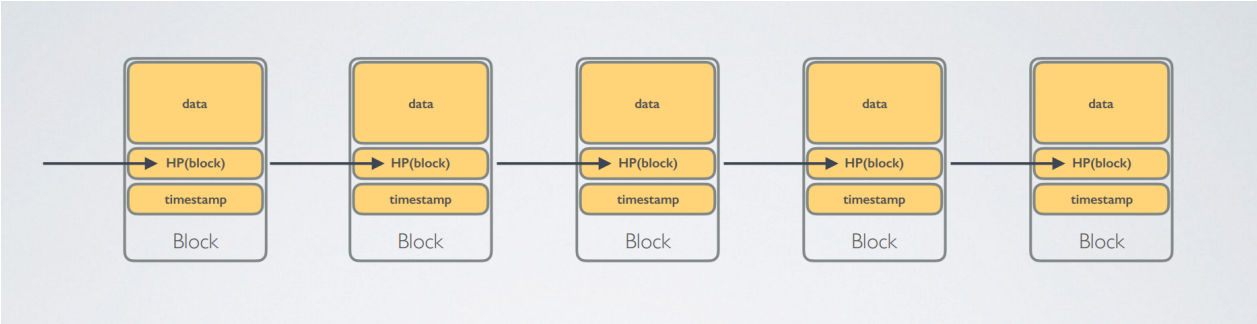


Figure 2: Blockchain data structure [14]

The hash value in the block header is calculated by the hash function based on the block information. Because of the “Longest chain principle”, changing the blockchain requires the attacking node to have more than half of the nodes in the network, so that the length of its pseudo-chain exceeds the length of the main chain, which is impossible in the real world. Therefore, it can be said that the data on the blockchain cannot be tampered with [16].

2.1.3 Traceability

The blockchain is a highly transparent and open system, where data broadcast across the network can be accessed and used by anyone through open access. According to this principle, any data on the chain can be traced back and blockchain can provide the location of historical data [16].

2.2 Cryptography

The security of the blockchain data layer strongly relies on cryptography-related technologies. Information encryption is a key part of a blockchain, and its algorithm mainly contains two parts: asymmetric encryption and hash function [17]. The asymmetric encryption part uses a private key to prove node ownership, which is achieved through digital signatures. A hash hashing algorithm to transform an arbitrary length input into a fixed-length output consisting of letters and numbers, which is irreversible and tamper-proof. The Bitcoin blockchain is a variant of the hash chain [3].

2.2.1 Hash Function

A blockchain can be called a "chain" because the cryptographic hash function forms a chain of pointers that links a series of blocks, each containing data and a pointer to a standard previous block. The pointer to the previous block uses its hash value, which is stored in the latter block to make it easier to find its location. The hash also serves to verify that the data contained in the block has not changed. Cryptographic hash functions are also used in the storage of the underlying data structure of the blockchain for ease of retrieval. A hashing

algorithm or a hash function is a cryptographic tool that compresses a message of arbitrary length into a fixed-length output value in a finite and reasonable amount of time. The hash function can be represented as:

$$H(x) = y$$

Its calculation is irreversible. The output value is called a hash value. Hash functions can be used in digital signatures, as well as in proving cryptographic security regimes, designing multiple cryptographic regimes and secure communication protocols as secure components.

Common hash algorithms are MD5 (Message Digest Algorithm) [18] with the output hash is a 32-bit hexadecimal number. MD5 was originally used for cryptographic hashing, while the possibility of its collision became greater with the increased number and computational power of computers. It is now commonly used as a common hash which is used for data verification. SHA (Secure Hash Algorithm) [19] is an advanced hash function used instead of MD5. Its output hash is a 64-bit hexadecimal number, which is considered impossible to crack because of the exceptionally large address space. It is used in Bitcoin [3]. the hash function should satisfy the following characteristics:

1. **Collision resistance:** It should be difficult to find two different inputs so that their outputs have the same hash value.
2. **Irreversibility:** It is difficult to reverse the calculation of the corresponding input value based on the output hash value (input hiding).
3. **Input Sensitivity:** The hash value of the computed output is completely different even if there is a small change in the input value.

The hash function is puzzle friendly, with no memory of the input. Bitcoin mining is the process of finding a target value that satisfies the conditions by changing the random number in the input value and continuously hashing the operation [3].

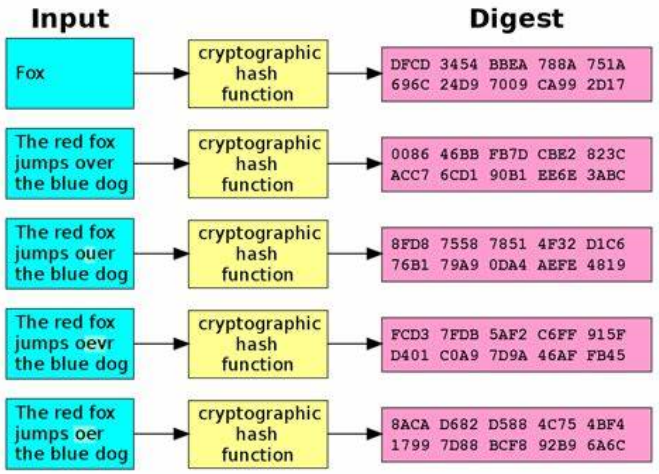


Figure 3: Calculation Procedure of the Hash Function

2.2.2 Encryption

Encryption algorithms are used to ensure the security and privacy of data during data transmission. The sender encrypts the file before sending it, and only the ciphertext is transmitted over the network to reduce the risk of being stolen by hackers. Symmetric encryption algorithms use the same encryption key and decryption key. The sender uses the key to encrypt the original file and sends it out, the receiver receives the ciphertext and needs to use the same key as the sender to decrypt the original text, this method requires the receiver and sender to agree in advance that both parties take the same key, which does not guarantee the uniqueness of the key owner. This algorithm requires each party that needs to carry out data transmission to have the same set of keys, which increases the number of keys and creates a key management burden when the number of users increases [20]. Common symmetric encryption algorithms include DES and RC5.

Symmetric encryption is not sufficiently secure because the key in symmetric encryption is transferred using the Internet between parties and asymmetric encryption appears. In an asymmetric encryption algorithm, each participant has two keys, a public key, and a private key. In the process of data transmission, the receiver needs to disclose his public key to the sender. The sender will encrypt the data to be sent using the receiver's public key, and then send the ciphertext to the receiver. After the receiver receives the ciphertext, he needs to use his key to decrypt and read the data. In the whole process, once the data is encrypted with the public key, only the corresponding recipient's key can decrypt the data, which greatly ensures security. Commonly used asymmetric encryption algorithms include RSA and ECC (Elliptic Curve Cryptography) [21]. Figure 4

shows the procedure of using the asymmetric encryption method and digital signature to generate a data transmission.

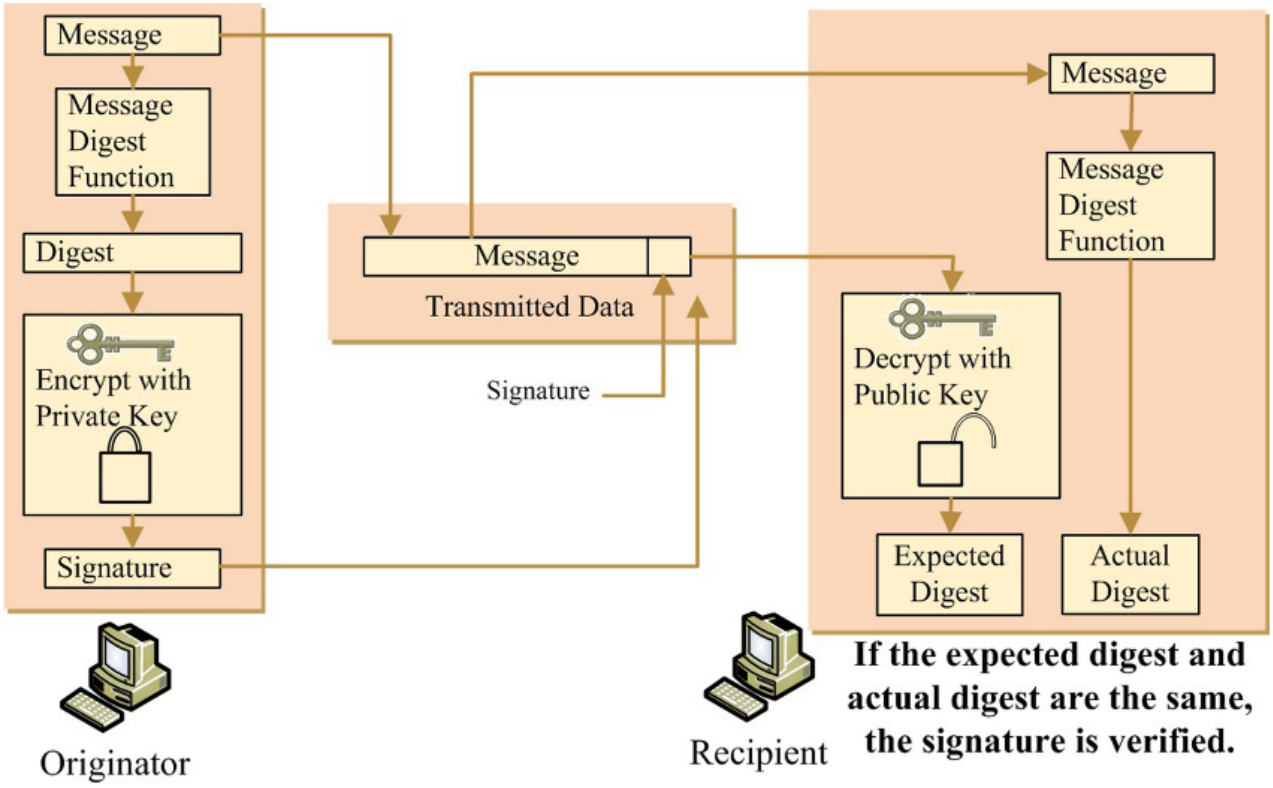


Figure 4: Data security digital signature process[22]

2.3 Blockchain in storage systems

With the rapid development of artificial intelligence and cloud computing, the scale of data storage is growing exponentially and there is a demand for storage technology with higher capacity, higher reliability, and lower latency than currently available systems [23]. Applying blockchain technology can improve the security and scalability of existing storage systems. The combination of blockchain and storage systems has caused two major changes:

1. Use of blockchain ledgers to store metadata for file slices [24].
2. Use of blockchain cryptocurrency as a reward to encourage users to actively provide storage space [25].

There are already many open-source decentralized storage projects based on the blockchain. The Interplanetary File System (IPFS) is a distributed file system that seeks to decentralize the web and make it faster and more efficient [26]. It was introduced in 2016 and is widely adopted by both individuals and

enterprise organizations. IPFS is primarily responsible for content discovery and content delivery in P2P networks, and Filecoin [25] is implemented as the incentive layer of IPFS, encouraging more nodes to join the IPFS network through value incentives. Because Filecoin is a decentralized system and implemented by blockchain technology, it can reduce storage space utilization in many cases.

To optimize the storage performance of existing systems by blockchain technology, Blockstack [27], a blockchain-based distributed internet was introduced in 2015, which focused on solving the single point failure of the DNS (Domain Name System) and the trust issues. It is a blockchain browser application that integrates decentralized data, decentralized applications, and decentralized user data. For large file storage scenarios, blockchain often requires an underlying file system to support it, using a combination of on-chain and off-chain storage. Zyskind et al. specified an approach for managing personal privacy information that Combines blockchain technology and file storage systems [12]. The specific principle is that store real files in the underlying file system, while public attribute information such as file summaries are stored on the blockchain, using the uniqueness and irreversibility of hash functions to verify data and manage access rights to files.

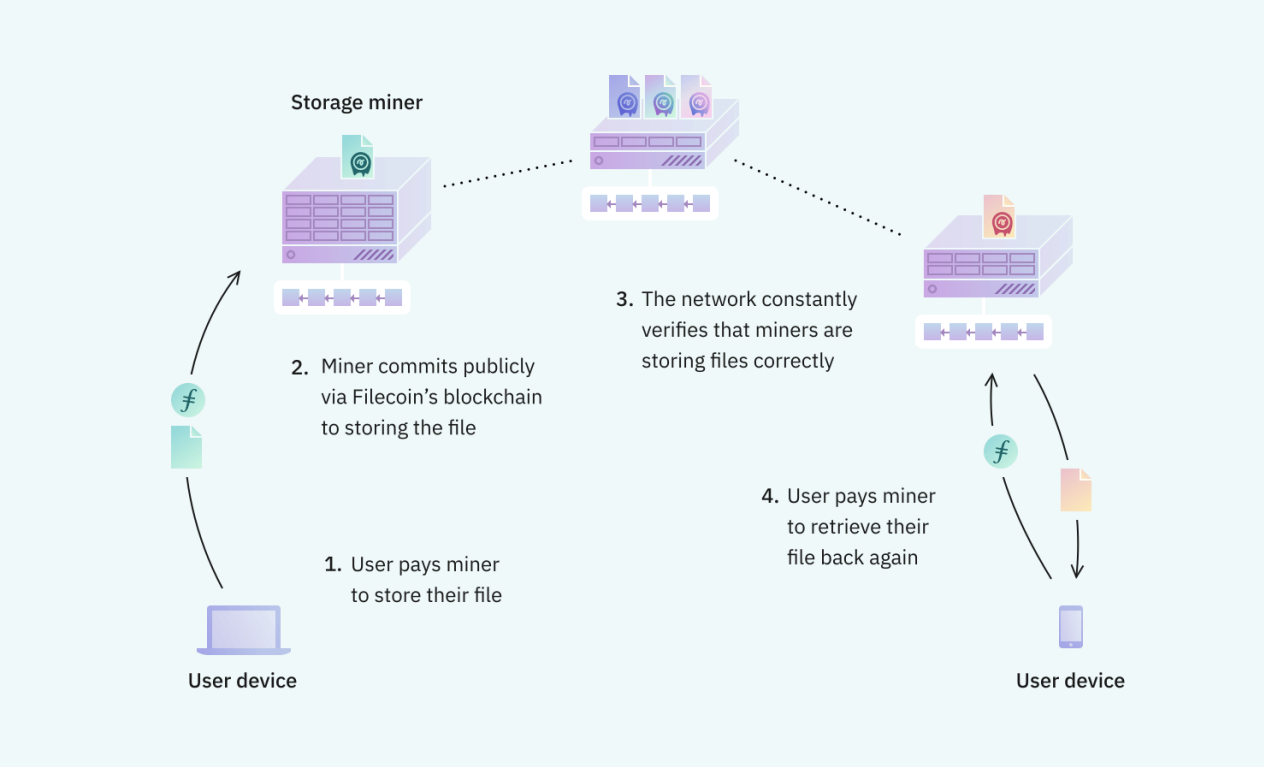


Figure 5: Procedure of storing and mining by Filecoin [25]

2.3 Blockchain in medical systems

Medical information in electronic medical records is managed by the hospital and, in past, patients did not have access rights. In addition, hacking of medical center facilities has been a frequent crime that leads to data extortion. Hospital and patient information have become increasingly insecure [28]. To solve these kinds of issues, Asaph Azaria from MIT designed and implemented a medical information sharing system combining medical blockchain and big data called MedRec [5] to maintain and manage the electronic Medical Record (EMR), using the Ethereum platform. While MedRec encourages medical stakeholders, medical institutions, patients, and researchers to participate in the Ethernet network as "miners", competing for arithmetic power to protect and maintain the Ethernet authentication logs, and being paid in tokens. Figure 6 shows the procedure of putting data onto the blockchain. Such consensus mechanism results in a certain amount of wasted computing power. Xhafa et al. [29] came up with another cloud-based medical records solution using symmetric encryption algorithms to prove the security of patients' and doctors' private information and detailed description of the diagnosis. Nevertheless, this system has the disadvantage of relying on a fully trusted third party called the Global Authority (GA) for key management, violating the idea of decentralization.

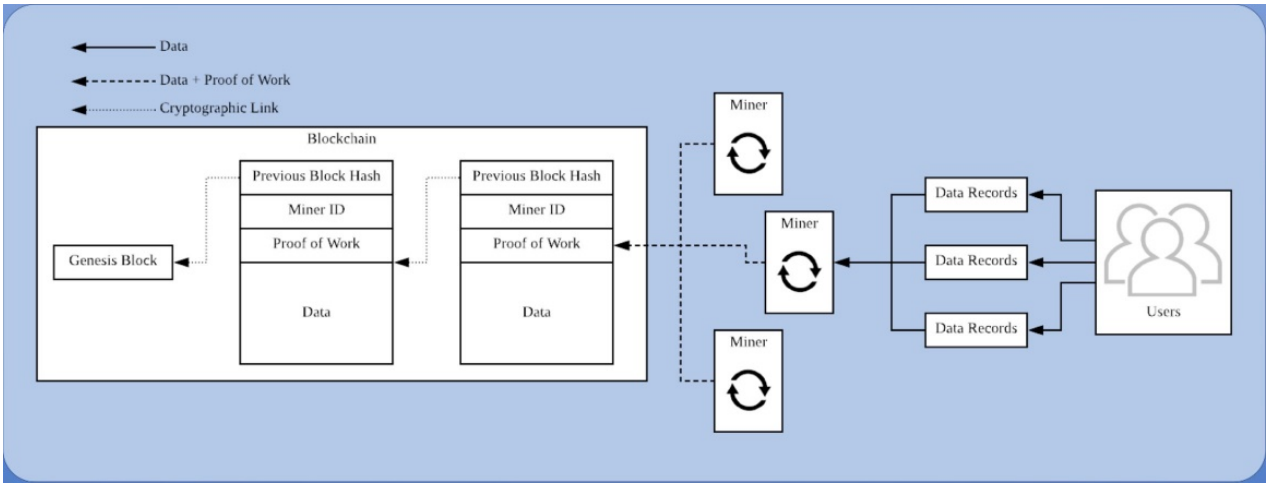


Figure 6: Method of putting the data on the blockchain using PoW Mechanism

As an improvement, an advanced service framework (ASF) for sharing medical records was presented by Chen et al. [30]. Compared with the traditional systems, it does not depend on a trusted third party. There are also some proposed scenarios of blockchain applications in healthcare based on these medical blockchain

system prototypes This work introduced a framework for primary care of oncology patients under cancer treatment [31]. The prototype they developed in collaboration with the Department of Radiation Oncology has been applied in a major US hospital. In China, medical blockchain mostly rests on theoretical models. Mei Ying et al. [32] combined blockchain and cloud storage technologies to propose a health chain for secure storage and sharing of personal medical records. In this system, public information, anonymous identities, and access rights to medical records are stored on the chain, while real medical data are encrypted and stored in an off-chain storage structure. It effectively achieves patient control over ownership and access rights to personal medical data and secure storage of sensitive medical data.

3 Methodology

This section introduces the research methodologies for all parts of the project.

3.1 Research Methods

In the early stage, I was not familiar with the blockchain and medicine. Papers that introduce the technologies and algorithms were selected as the primary references in that stage. After having a preliminary understanding, I started collecting research papers that specify existing approaches and solutions in the field of medical blockchain. I evaluated the advantages and disadvantages of their prototypes or designed systems became the research method in the system design stage. When we completed the initial system prototype, the research direction came to medical measurement and report a protocol for a case study, which could provide a specific usage of our system and help us know the procedure of data transfer in the real world with considering realistic factors. Because this is a design and implementation project, the research and analysis alone are not sufficient. Following the research and design stages, the implementation (development) is a software engineering component of this project that also serves as the proof of concept.

3.2 Software Engineering

I strictly followed agile project management methods: individuals and interactions over processes and tools, working software over comprehensive documentation, customer collaboration over contract negotiation, responding to change over following a plan [33]. Its two most important features are lightness and simplicity. Agile methodologies involve minimal processes and documentation and reduced formality. The aim is to do what can be done in the immediate future, without predicting too far into the future, and to get the urgent things done first. The reason I chose this methodology is that this project requires to design and implement a new system and no existing solution. I need to collect requirements and communicate with the supervisor to check and update the design ideas. In that condition, frequent meetings and modifications made the long-term schedule with very detailed system specifications impossible. The software engineering strategy I chose is FDD (Feature-Driven Development) [34]. Feature-Driven is essentially Model-Driven, where a complete Domain Model is planned as the starting core of the system. In the traditional waterfall model, we tend to see the delivered features only after subsequent coding has been completed while we could finish more iterations and give rapid deliveries in FDD. This strategy generally contains these five steps:

1. Develop an Overall Model
2. Build a Features List
3. Plan By Feature
4. Design By Feature
5. Build By Feature

3.3 Systematic Mapping Study

Systematic mapping study (SMS) focuses on providing an overview of a field, identifying research evidence on a topic, and providing quantitative (primary) and qualitative data [35]. The objectives and research questions are the most important aspects of the overall systematic mapping study. According to the principle of SMS, these problems should be considered:

1. Why should I do this thing?
2. Did anyone do the same or similar thing?
3. Is it an appropriate time now?
4. What is the research exactly?

4 Design

This chapter introduces the design ideas of each component in the medical blockchain system, kernel encryption method and transaction procedure. The design was based on some relevant prototypes and existing achievements in Prof. Brusic's Smart Health Home project.

4.1 Requirement Specification

This section states the requirements of this project. The specifications of requirements could be divided into two types: functional and non-functional. Functional requirements define what the system should do, while non-functional requirements display how the system works [36]. The software requirements below are applicable for the whole medical blockchain system application. The UML diagram could be seen in the Appendix.

4.1.1 Functional requirements

Data Content

1. Medical data should be processed by an edge computer, which means the encrypted data is a simple report or summary but not all the details received by smart home sensors.
2. There is also a pointer that points to the concrete details of body data stored in the block.
3. Patients could upload medical data and download health reports.
4. Doctors could upload health reports and download medical data.
5. The health report should have types and contain a certain type of medical data measurement.
6. The user need not upload the report to the blockchain directly.

Security

1. The real personal information (identity) is anonymous.
2. User could not change the medical data and historical diagnosis but could update body information.
3. Doctor could only access the data with the patient's agreement.
4. institutions like a hospital could store the open medical data in their block.
5. The access from doctors or medical institutions to a health report should be recorded.

Credits (Advanced function if time is enough)

1. Users have accounts with credits.

2. Users could set the public access to their data and gain credit by providing medical data.
3. Hospitals could gain credit for data sharing or pay credit for medical data for experiments.

4.1.2 Non-functional requirements

Performance

The performance could be divided into two parts: stability and response time. The medical blockchain system should have good performance for data uploading and transaction updating. Every node should be unblocked on blockchain and all the querying and invoking operations in the ledger should be in a limited time.

Portability

The blockchain system could be transplanted to a different environment. This means this system need a unified installation procedure in different machine ignoring the version of the operating system and dependencies.

Usability

The blockchain system should be easy to operate for both the patient side and the doctor side. It contains a simple interface and clear guidance. The interactions with the blockchain systems should be automatic and not bring many Learning costs for users.

4.2 System Design

The scope of this Medical Blockchain project is to provide a trusted environment with privacy protection and data encryption for transferring personal health reports from the data exchange center to doctors or other health partitioners. When a patient or doctor requests a visit or a doctor requests home health care information, a suitable report will be generated. Such data include may include reports containing heart rate, blood pressure, blood glucose level, weight, activity, sleep, ECG, or others. The report should be readable, contain meaningful information and be organized in a manner that enables the healthcare practitioner to receive the critical information fast in a format that is easy to read and interpret. The block diagram in the figure below shows the interactions between each component of the system.

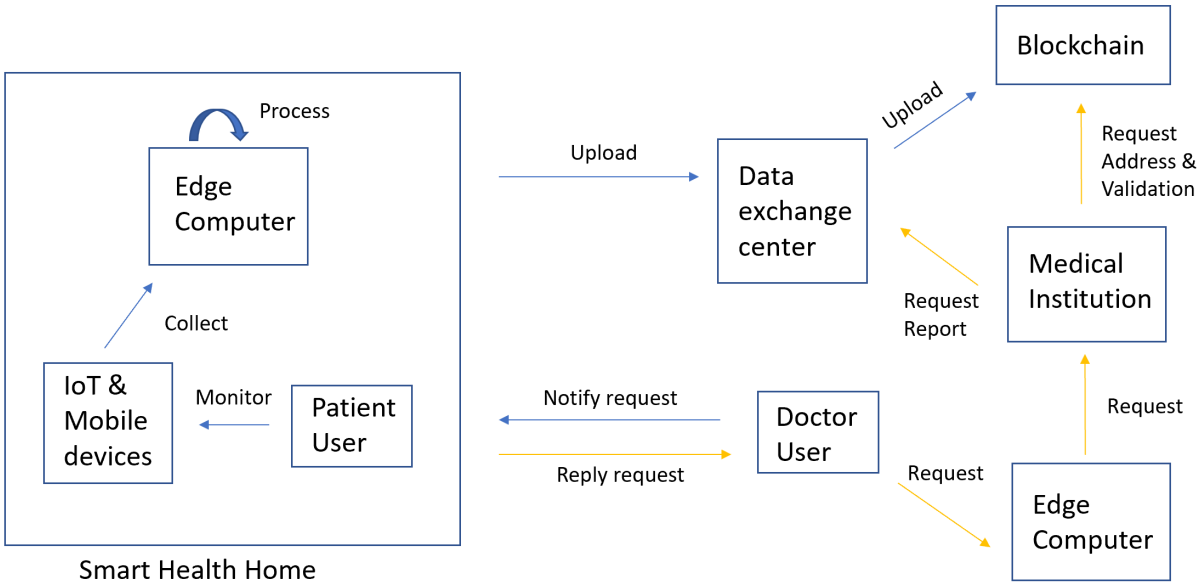


Figure 7: Block diagram of the medical blockchain system

A framework is proposed for managing and transmitting medical raw data and reports extracted from wearable devices by edge computers, for medical monitoring support (Figure 5). This framework should provide a trusted environment for data exchange between Smart Health Homes and medical institutes with privacy protection and data encryption. The proposed system must ensure:

- correct data are collected
- data accuracy is assured
- data are anonymized before sending and correctly re-identified at health care institution
- transaction records are immutable

Data pre-processing and the method of data uploading to the blockchain are crucial parts of this system. The system should allow handling of the raw data, as well as sharing of key information in the form of reports or summaries. The type of report depends on the health conditions, and it must provide meaningful information. The data in the report must be medically certifiable to satisfy medical use standards – we developed a proposal for an industry standard for medically certifiable blockchain transfer.

4.3 Smart Contract

The concept of smart contracts was first introduced in 1997 by cryptographer Nick Szabo [37], who wanted to eliminate the middleman and have the contract take effect automatically as soon as certain conditions were met.

4.3.1 Overview

The advent of blockchain technology has driven the development of smart contracts. A contract is a computer protocol in the form of code with no third party required. It is essentially a computer program written by a programmer and stored in a block, using deterministic algorithms and a defined data source, and satisfying terminability. When the state of the network changes to meet the initial conditions set, the "miner" will automatically execute the contents of the smart contract. Ethereum and Hyperledger Fabric are two representative technology platforms for the application of smart contracts, and the Table in Figure 5 briefly compares them in terms of consensus mechanism and programming language.

		Ethereum (Public)	Hyperledger Fabric
Infrastructure	*Nodes*	Running Ethereum client	Peers and Orderers, plus other supporting nodes
	Ledger	Kept in every node	Kept in Peers
	Block Building	Through mining. Any nodes can be mining nodes at one's own wish.	Orderers build the block
	Consensus	Mining nodes send out valid block, and all nodes follow the rule of accepting block locally.	Orderers send out block after consensus, and Peers commit the block into local ledger.
	Native Currency	Ethers, acting as economic incentive for the nodes maintaining the network	Not applicable. Each node is responsible for maintaining network robustness
	Contract Code Execution	Inside Ethereum Virtual Machine (EVM) on each node	Predefined Endorsing Peers according to business policy
Application	*Contract Coding Language*	Solidity, Vyper	Go, Node and Java
	Client Application	Using libraries provided for various coding languages	Using SDK provided for various coding languages

Table 1: Comparison of Ethereum, Hyperledger Fabric [38]

Smart contracts enhance the flexibility of blockchain technology for application in real business scenarios. Like traditional contracts, legal terms are implemented in code, programming complex relationships between

people and using computer programs to establish prestige and binding force. It is important to note that as smart contracts are automatically executed and do not allow third-party intervention, the reasonable design and operation of the contract content is the key to the stable operation of the whole system, and if there are problems with the logic in the contract code, the security of the blockchain will be seriously affected. Therefore, smart contracts need to be carefully checked in advance before they are uploaded to the chain.

4.3.2 Smart Contract Design

In the smart contract, only the kernel functionalities should be included. To make the smart contract elegant and efficient. The designed on-chain data is health report entities, and the report access records and all the other functionalities should be removed from the blockchain. We designed the smart contract that allows the patient to upload medical health reports by proxy of the data exchange center and the doctor to access the report on-chain by hospital nodes. There are three types of actors for identification: administrator, medical institution, and data exchange center. And the smart contract provides three kinds of functionalities: authentication, report uploading, and report query. The data flow during the transmission is shown in the figure below:

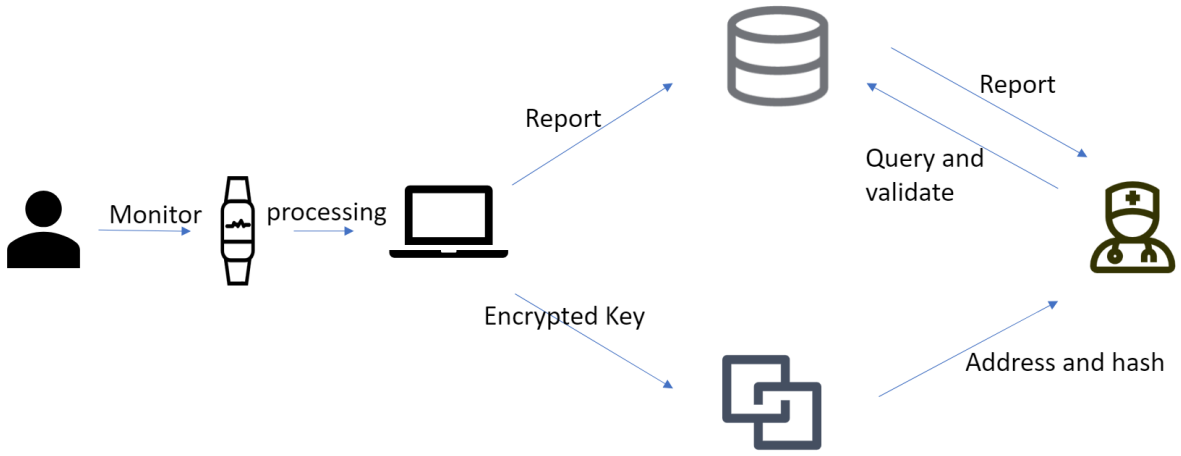


Figure 8: Data transmission flow in the medical data sharing system

4.4 Encryption Method

To ensure the privacy and security of blockchain, there is a widely used encryption method according to the existing double encryption solution by combining symmetric and asymmetric encryption. Firstly, it uses sha256 random algorithm [39] to generate a private key and the ECC algorithm [40] to calculate the corresponding public key for every user (patients and doctors). The private key should be stored by the user himself and could not be known by anyone other and the public key can be seen by all the other users in this blockchain system. When a patient prepares to share a medical report with the doctor, the report file will be encrypted by the Advanced Encryption Standard (AES) algorithm [41], which is a symmetric encryption algorithm on an edge computer. Then the generated AES key will be secondly encrypted by the RSA algorithm [42] with the doctor's public key. This step is to ensure that only the doctor he chooses can decrypt the AES key using his private key. After that, the patient-client will also generate a hash digest from the report file and use his private key to make a digital signature. This step is on purpose to ensure that the report file is not changed maliciously. The Ciphertext of the report itself will be sent to the data exchange center. The exchange center will generate a pointer or address for querying the report. Both this address encrypted AES key, and hash digest with signature, these three things will be uploaded on the blockchain, and everyone could access these ciphertexts on-chain.

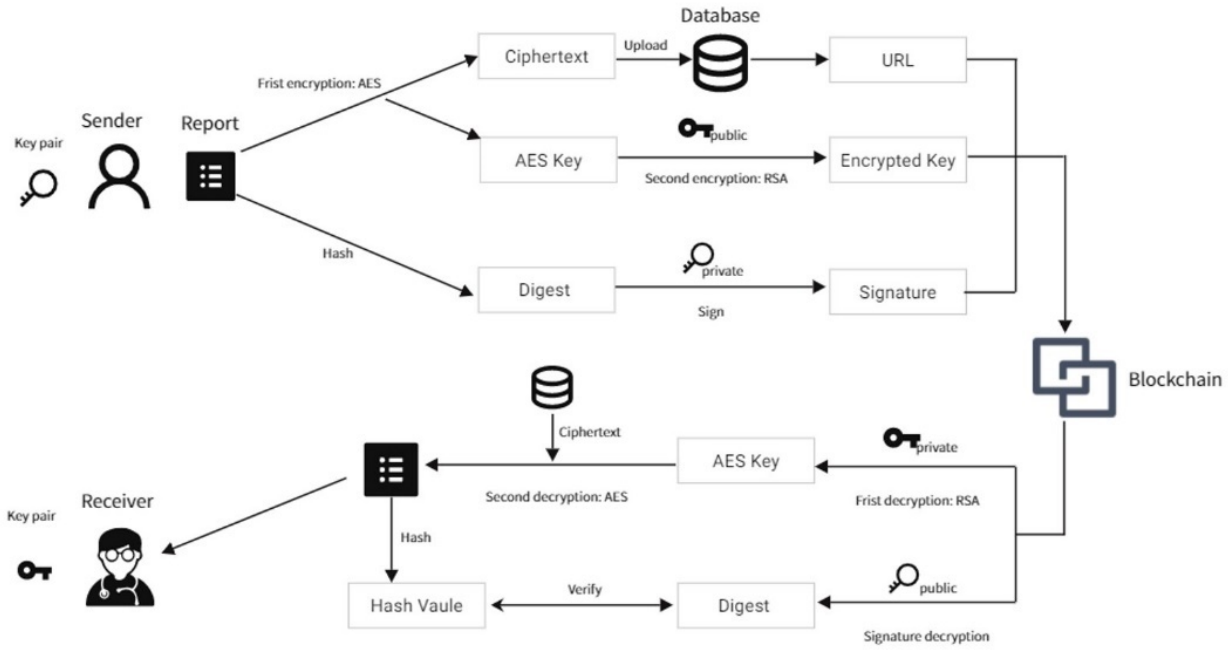


Figure 9: Common Encryption Procedure in the blockchain system

The doctor could query the blocks by a patient public key and get all these ciphertexts. Then he needs to use his private key to decrypt the AES key and use the decrypted AES key to decrypt the report ciphertext. The final step to complete all this procedure is using the patient's public key and hash digest in block to verify if the report is changed.

In our proposed medical blockchain system, we removed this encryption of data reports and vulnerable information in the diagram (AES symmetric encryption). Because the health report is anonymous, risks of data leakage could be reduced. We designed to allocate a unique ID for each health report and bind the report with a patient's public key. When a patient wants to share a piece of the report with a doctor, he needs to use his private key for a digital signature and the doctor's public key to bind with his uploaded report. This step provides the access rights to his doctor.

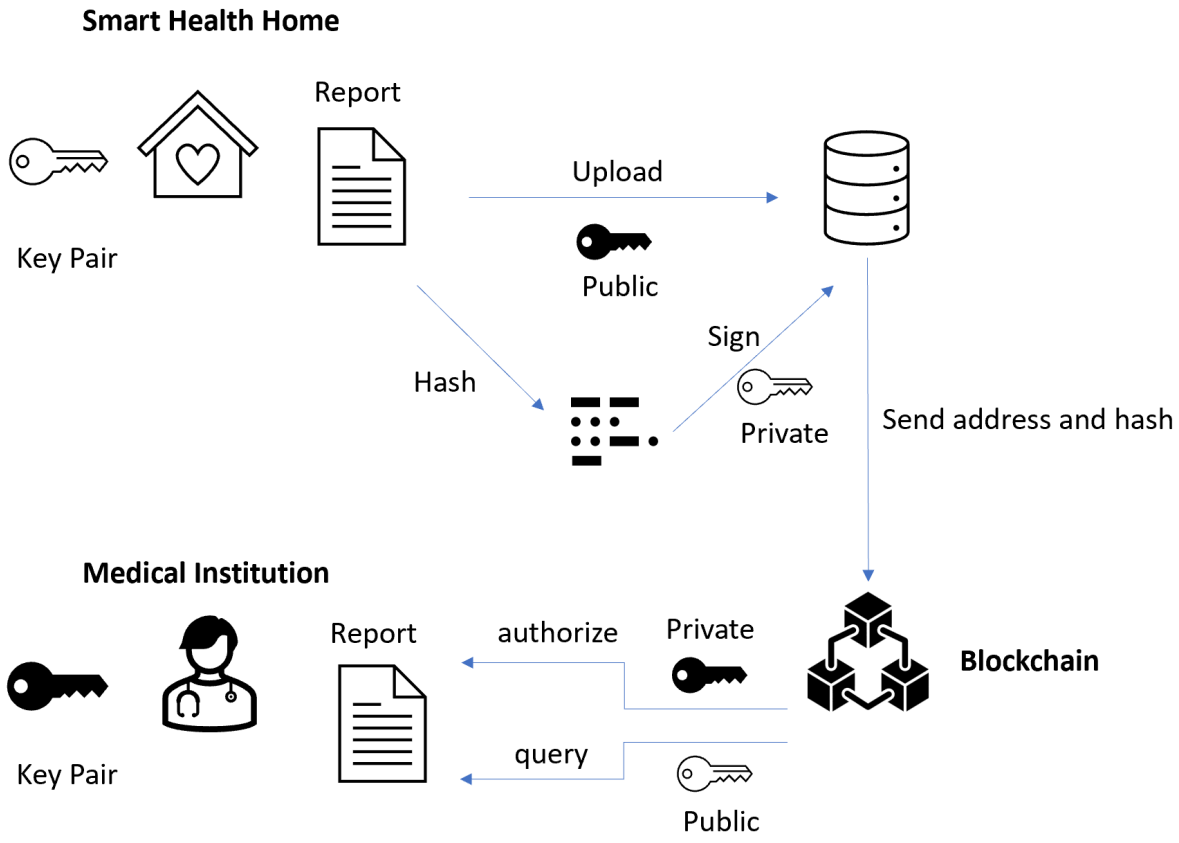


Figure 10: Encryption Procedure in our blockchain system

4.5 Transaction Procedure

The procedure of a complete medical report transfer could be seen in Figure 7. This event is generally requested by the doctor. When a doctor needs to see the current situation of his patient, he will send it to the hospital using his edge computer in the office and the hospital server will collect all the requests from doctors in the hospital and upload requests on the blockchain as a full node. Then blockchain system will notify the patient-client. After the patient's approval, his edge computer will follow the medical report according to the doctor's assigned format and protocol to make a measurement. The medical report will be generated later and automatically finish the transfer to the exchange center. The smart home is a light node, which means it could only execute query operations on blockchain but not upload operations. The data exchange center is another important full node on a chain with Authorization from the whole medical Alliance. It will permanently store the user's report and finish the uploading operation by following the encryption steps in 5.2. The necessary digest and address are on-chain for doctor's verification. Then blockchain system will report the status of the report submission and the hospital would find that. The doctor will receive a message of report arrival soon and the whole procedures of a transaction completed now.

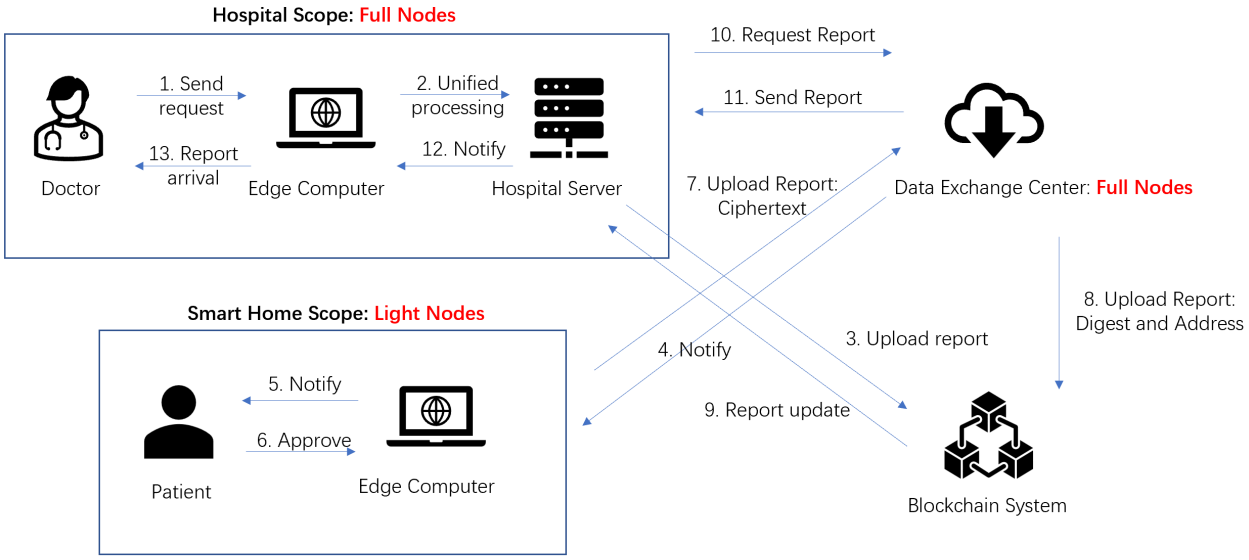


Figure 11: Sequence diagram of finishing a complete transaction of medical report transfer

4.6 Blockchain Transfer Protocol

Health data contains many types. After considering the conditions of our smart health home prototype and doing research, we design the protocol of transfer. The system allows the user to transfer these data types: **heart rate, blood pressure, body weight** (maybe accelerometer data and ECG). For simple data, its original format could be uploaded on chain; while for these long-term monitoring data with big sizes, the blockchain system only stores a hash value for validation and an address to the DEC (Data Exchange Center). Here are two examples of transferred data introduced below, which are blood pressure and body weight.

4.6.1 Blood Pressure

Background

Hypertension is the leading risk factor of mortality in China, accounting for 2·54 million deaths in 2017 and most were due to cardiovascular diseases. It was estimated about 23.2% (244.5 million) of Chinese adults had hypertension, the awareness and treatment rates are 46.9 and 40.7% respectively, and only 15.3% were controlled [43]. The 2018 Chinese hypertension guidelines highlight that accurate BP measurement is fundamental for assessing BP levels, establishing the diagnosis of hypertension, and evaluating the efficacy of antihypertensive treatment.

BP category (mmHg)	CHL 2018 [1]	KSH 2018 [7–9]	JSH 2019 [10]	AHA/ACC 2017 [2]	ESC/ESH 2018 [3]
SBP < 120 and DBP < 80	Normal	Normal	Normal	Normal	Optimal
SBP: 120–129 and DBP < 80	High normal	Elevated	High normal	Elevated	Normal[a]
SBP: 130–139 and (or) DBP: 80–89		Prehypertension	Elevated	Grade 1 hypertension	High normal[b]
SBP: 140–159 and (or) DBP: 90–99	Grade 1 hypertension	Grade 1 hypertension	Grade 1 hypertension	Grade 2 hypertension	Grade 1 hypertension
SBP: 160–179 and (or) DBP: 100–109	Grade 2 hypertension	Grade 2 hypertension	Grade 2 hypertension		Grade 2 hypertension
SBP ≥ 180 and (or) DBP ≥ 110	Grade 3 hypertension		Grade 3 hypertension		Grade 3 hypertension
SBP ≥ 140 and DBP < 90	ISH	ISH	ISH	NA	ISH

ACC American College of Cardiology, *AHA* American Heart Association, *BP* blood pressure, *CHL* Chinese Hypertension League, *DBP* diastolic BP, *ESC* European Society of Cardiology, *ESH* European Society of Hypertension, *ISH* isolated systolic hypertension, *JSH* Japanese Society of Hypertension, *KSH* Korean Society of Hypertension, *NA* not available, *SBP* systolic BP.
[a] DBP: 80–84 mmHg
[b] DBP: 85–89 mmHg.

Table 2: Blood Pressure Classification guidelines from BP categories in Chinese, Korean, Japanese, US and European hypertension guidelines [44]

Blood Pressure Measurement

To develop a proposal for an industry standard for medically certifiable blockchain transfer, we need to research the whole measurement procedure of blood pressure. The steps below are what we concluded from blood pressure measurement guidance [44].

- 1. Refrain from smoking or ingesting caffeine for 30 minutes before measurement.
- 2. Be seated quietly for at least 5 minutes in a chair (rather than on an exam table).
- 3. Keep feet on the floor, and arm supported at heart level.
- 4. Use the equipment that satisfies the standard of blood pressure.
- 5. Choose the appropriate size cuff

The medical report should contain measured timestamp, measure results (systolic and diastolic BP, if it is a daily report, there will be two measurement results, morning measurement and evening measurement; if it is a weekly or monthly report, there will be two charts that reflects each measured result and trend of data). The report file could be organized in JSON format which is convenient for transfer.

4.6.2 Body Weight

Background

Bodyweight could reflect the health conditions. The figure below shows the health range of BMI. Underweight and overweight are significant evidence to diagnose dystrophy and obesity respectively. Obesity causes or exacerbates many health problems, both independently and in association with other diseases1. It is associated with the development of type 2 diabetes mellitus, coronary heart disease (CHD), an increased incidence of certain forms of cancer, respiratory complications (obstructive sleep apnoea) and osteoarthritis of large and small joints.

BMI* (kg m^{-2})	WHO classification	Popular description
<18.5	Underweight	Thin
18.5–24.9	—	'Healthy', 'normal', 'acceptable'
25.0–29.9	Grade 1 overweight	Overweight
30.0–39.9	Grade 2 overweight	Obesity
≥40.0	Grade 3 overweight	Morbid obesity

*BMI is the weight in kilograms divided by the square of the height in metres.

The data presented in Tables 1 and 2 reflect knowledge acquired largely from epidemiological studies in developed countries. Preliminary information from developing nations indicates that lower cut-off levels for both BMI and waist circumference (see Table 2) are necessary for certain populations who are at particular risk from comparatively modest degrees of overweight.

Table 3: Cut-off points proposed by a WHO expert committee for the classification of overweight [45]

Another important usage of body weight is monitoring the health conditions of pregnancies. The doctor could analyze the body weight gains and take health care of pregnancies [46].

	Total Weight Gain		Rates of Weight Gain* 2nd and 3rd Trimester	
Prepregnancy BMI	Range in kg	Range in lbs	Mean (range) in kg/week	Mean (range) in lbs/week
Underweight (< 18.5 kg/m^2)	12.5-18	28-40	0.51 (0.44-0.58)	1 (1-1.3)
Normal weight (18.5-24.9 kg/m^2)	11.5-16	25-35	0.42 (0.35-0.50)	1 (0.8-1)
Overweight (25.0-29.9 kg/m^2)	7-11.5	15-25	0.28 (0.23-0.33)	0.6 (0.5-0.7)
Obese (≥ 30.0 kg/m^2)	5-9	11-20	0.22 (0.17-0.27)	0.5 (0.4-0.6)

* Calculations assume a 0.5-2 kg (1.1-4.4 lbs) weight gain in the first trimester (based on Siega-Riz et al., 1994; Abrams et al., 1995; Carmichael et al., 1997).

Table 4: Recommendations for total and rate of weight gain pregnancy, by pregnancy BMI from Weight gain during pregnancy: reexamining the guidelines [46]

Measurement

Here are the requirements of body weight measuring preparation:

1. Setting up the measurement site: the scale should be placed on a hard-floor surface (not on a floor that is carpeted or otherwise covered with soft material).

2. Calibration of scale: calibration should occur at the beginning and end of each examining day. The scale is checked using the standardized weights and calibration is corrected if the error is greater than 0.2 kg. The results of the checking and the recalibrations are recorded in a logbook.

The user in the smart health home should follow the steps below to make the bodyweight health report accurate:

1. Participants are asked to remove their heavy outer garments (jacket, coat, trousers, skirts, etc.) and shoes. If subjects refuse to remove trousers or skirts, at least make them empty their pockets and record the fact in the data collection form (see textbox 6.2).
2. The participant stands in the center of the platform, weight distributed evenly to both feet. Standing off-centre may affect the measurement.
3. The weights are moved until the beam balances (the arrows are aligned). (This concerns the balanced beam scale only).
4. If the person's weight exceeds the maximum of the scale, the self-recorded weight is acceptable and recorded on the collection form.

The health report should contain a measured timestamp, and measure results (the average value of three measurement results, age, and height). The report file could be organized in JSON format which is convenient for transfer.

5 Implementation

This chapter introduces the implementation of the blockchain system, which contains technical details, different development stages and current results of this project.

5.1 Hyperledger Fabric

5.1.1 Overview

Fabric is a modular and extensible open-source system for deploying and operating permission blockchains and one of the Hyperledger projects hosted by the Linux Foundation [47]. It is the first truly extensible blockchain system for running distributed applications. It supports modular consensus protocols, which allows the system to be tailored to particular use cases and trust models. Fabric system also supports running distributed applications written in standard, general-purpose programming languages, without systemic dependency on a native cryptocurrency. Authors demonstrated that Fabric accomplishes end-to-end throughput of more than 3500 exchanges per minute in certain prevalent sending arrangements, with sub-second inactivity, scaling well to over 100 peers.

Unlike Bitcoin [3] and Ethereum [48], Hyperledger Fabric network membership relies on Membership Service Provider (MSP) registration, rather than allowing anyone to participate in the network through PoW (proof-of-work) or PoS (proof-of-stake) mechanisms. Because of this feature, Hyperledger Fabric is widely used to build systems that need an alliance chain or private chain to prove privacy and security.

5.2.2 Technical Architecture

The flexible and pluggable component nature of the fabric relies on its highly modular structure. It includes three main components: Membership Servers (MSP), Blockchain Servers, and Chain code Servers. The overall functional architecture of the fabric is shown in the diagram below:

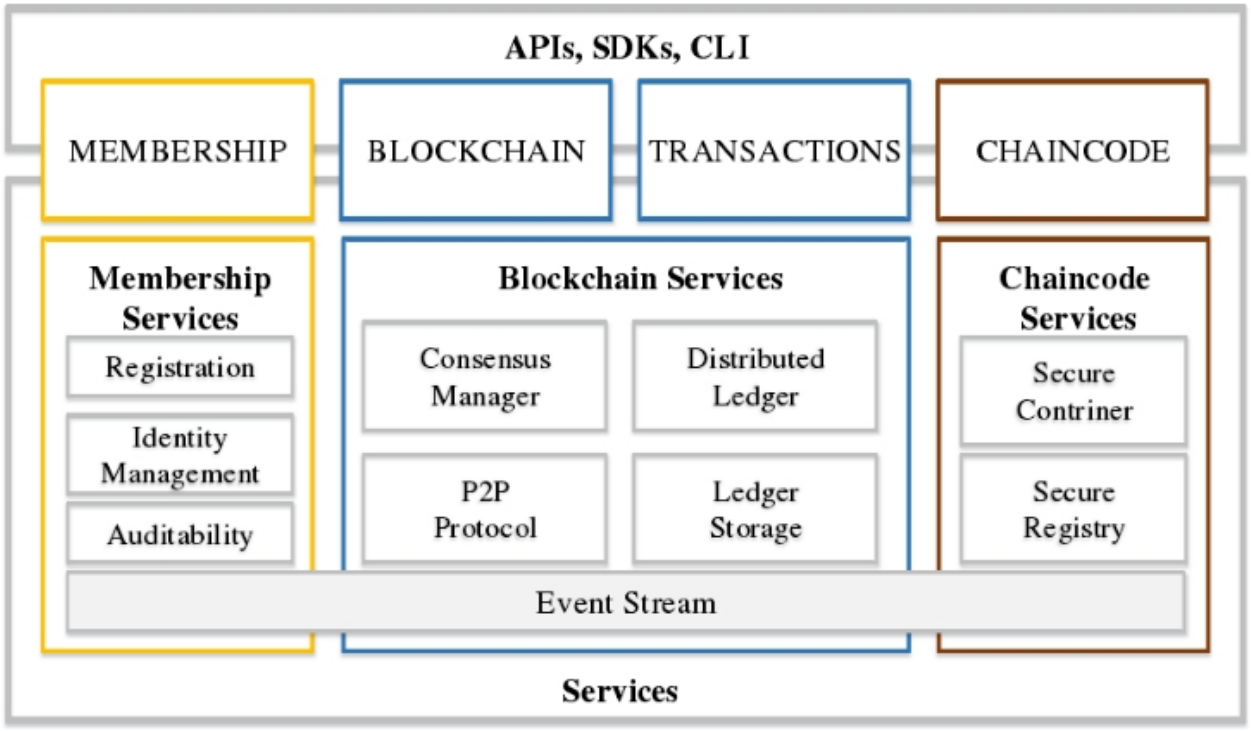


Figure 12: Hyperledger Fabric Architecture [47]

Membership Service Providers (MSP) are responsible for providing registration, identity management and audibility services for members. The Fabric federated chain provides a membership certificate management service through the MSP that determines which nodes on the chain are trusted, and all types of nodes and clients must be authorized by the MSP before they can join the network. The prerequisite for certificate authorization (CA) is the configuration of a Public Key Infrastructure (PKI), which is a set of technologies and specifications for a security infrastructure using standard public-key cryptography. CA certificates are divided into two categories, Root Certificate Authority (RCA) and Intermediate Certificate (ICA), which form a certificate trust chain [47].

Channel is a logical concept where nodes within the same channel can communicate with each other, and nodes cannot establish connections between themselves across channels. Each channel has a global MSP that manages the joining and exiting of nodes [47].

Blockchain Service includes services such as P2P Protocol, Consensus Manager, Distributed Ledger, and Ledger Storage [47]. The ledger consists of two parts: the Blockchain and the State. The Blockchain is a chain of connected blocks, used to record historical transactions; the State is a database in the form of a Key-Value, corresponding to the latest World State of the current network, which needs to be updated for each transaction on the same key.

Chain Code is a computer program written by the system developer and stored in a ledger, commonly referred to as a **smart contract** [47]. The chain code contains business logic code, which can be written in Go, Java, Node.js and other languages, and runs on a Docker container. Clients of different languages trigger the chain code by installing the corresponding software development kit (SDK) to call the application programming interface (API), and the chain code calls the corresponding function to execute the business logic and access the ledger to update the state of the world according to the parameters passed by the client.

5.2.3 Consensus Algorithms

Network nodes in a fabric blockchain are required to maintain the same ledger state across the network, and the nodes can essentially be seen as state machines that replicate each other. The Fabric achieves distributed node consistency through a consensus process, which can be seen as a transaction realization process, consisting of three stages, endorsement, ordering, and verification.

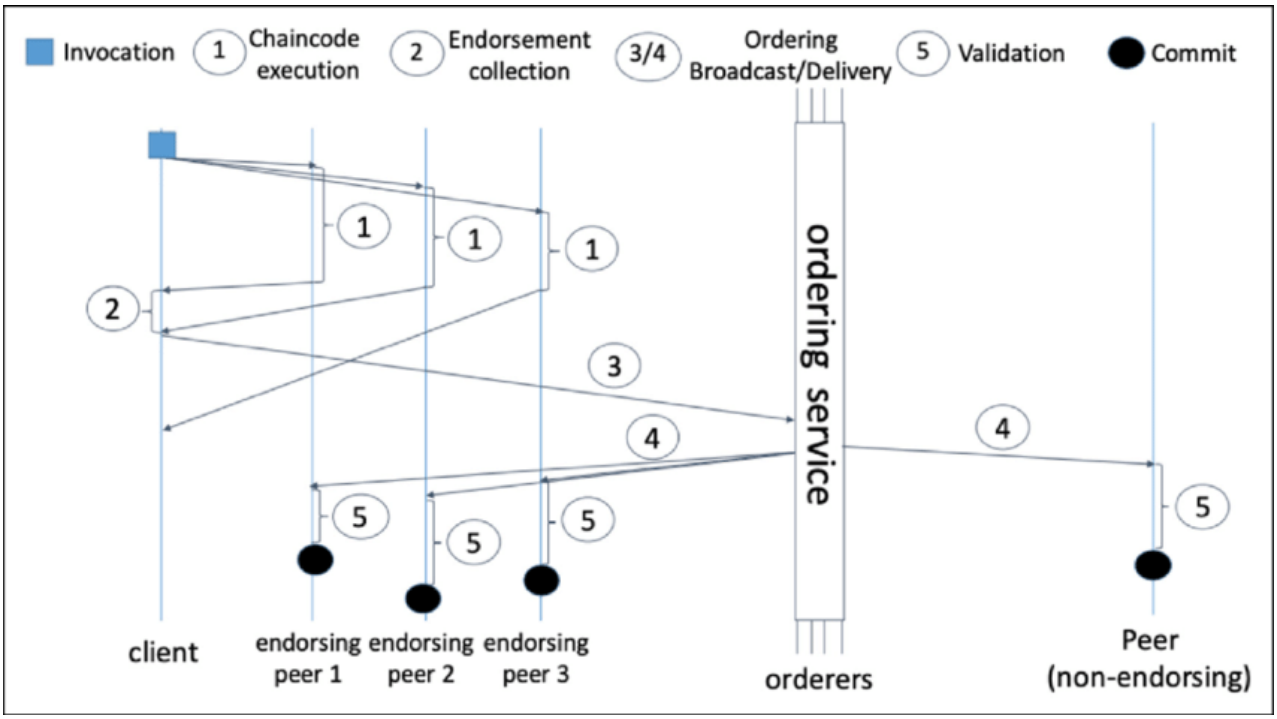


Figure 13: Transaction flow of Hyperledger Fabric

Endorsement: The client submits the transaction to the endorsing node, which verifies the signature of the received transaction proposal and simulates the execution of the chain code to get the result, after which the verification result, endorsement result and certificate signature are sent back to the client as the proposal result; according to the endorsement policy, the client does not consider the transaction valid until it receives enough feedback on the agreement of the proposal.

Ordering: The Ordering Service Node (OSN) sorts the transactions received over a period, packs the sorted transactions into data blocks and broadcasts the new blocks to the members of the channel.

Validation: The validation node performs a series of legitimate checks on the sorted transactions, including the correct signature, the integrity of the transaction data, and whether the endorsement policy is satisfied. After all transactions in the data, the block pass the checksum, the block is considered legitimate and written to the ledger, and then the Key-Value state database is changed [47].

5.2 System Architecture

The proposed medical blockchain system uses a Three-layer architecture which includes the backbone: a blockchain framework for kernel transaction dealing and privacy proving, a frontend for user interaction and visualization, backend for requests and responses dealing. The implementing architecture of this project will follow the figure below:

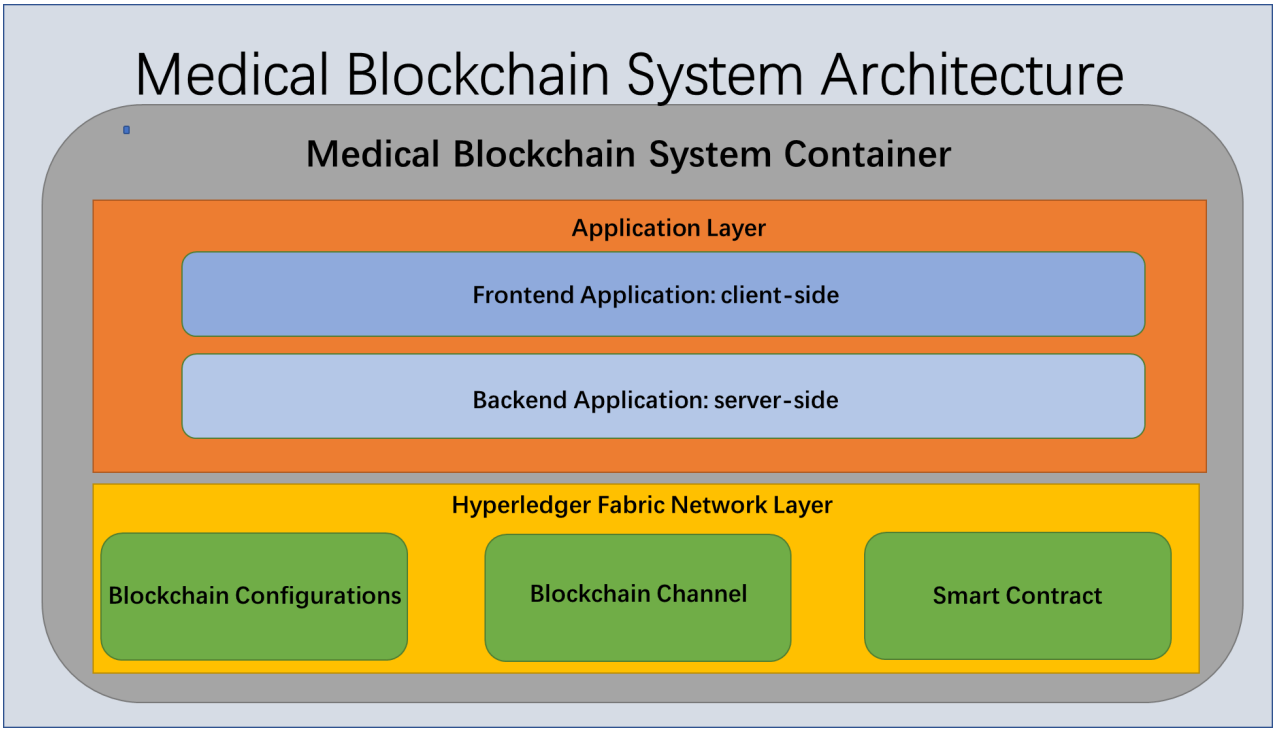


Figure 14: Architecture of our Blockchain System in Smart Health Home

5.2.1 Blockchain framework

This project uses the Hyperledger Fabric framework [47]. All the Fabric blockchain nodes run on the Docker container. Containerization helps developers to ignore the differences between machines and the environment.

We used the official testing network configuration to build the development environment and encapsulated the command line instructions into a bash script. When we start a network, the terminal will show content like the figure below. There are one orderer node, two organizations, and three peer nodes for each organization.

The Fabric will generate the genesis block and Certificates of nodes. After starting the blockchain network, a smart contract package could be deployed on the channel. We used Golang language to write the smart contract (called chain code in Fabric). Then we could run the invoke and query function in the smart contract on the channel. For example, a simple smart contract that shows body weight transfer is developed as a testing case. Ledgers in different nodes will be synchronized by the Fabric network.

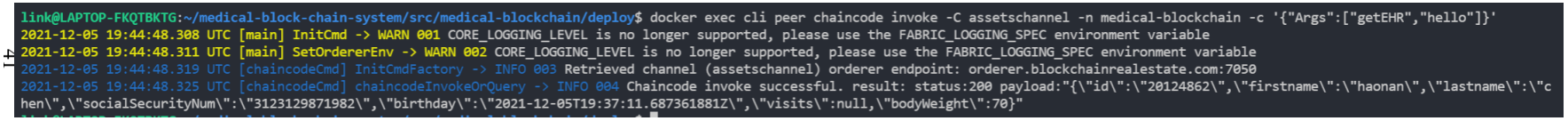


Figure 15: A simple smart contract that shows body weight transfer

5.2.2 Frontend

We use the Vue framework to develop the front end for user interactions and visualizations. In the log in the interface, we could now simulate multiple actors to create new measurements and send them to another user in this system.

Figure 16: The Login interface of the system

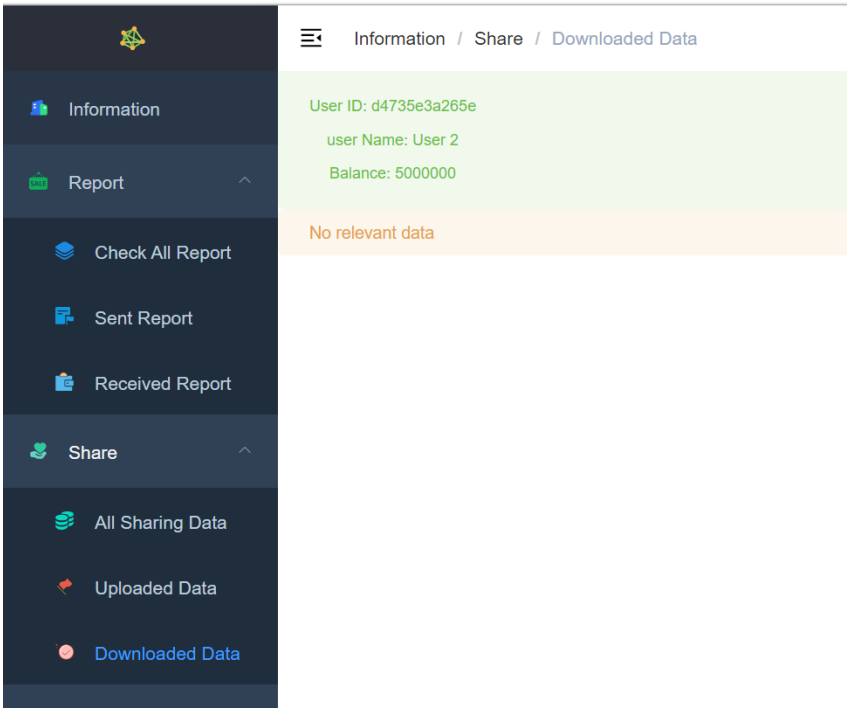


Figure 17: The front-end user interface

5.2.3 Backend

We used Golang and gim to develop the backend to deal with the requests of calling smart contracts. The gym is a very light web framework using Golang. It has the advantages of low memory usage and rapid response.

Figure 18: List of requests to the Backend and their response time

5.3 Blockchain Deployment

In this experiment, the Hyperledger Fabric v2.1 test network was used. It includes three organizations, org1 and org2, two peer nodes belonging to each organization, one order node, and one channel, “mychannel”. The fabric network deployment includes generating certificates for each organization, generating genesis blocks, creating channels, deploying contracts, etc.

The bash commands below show how to start a fabric blockchain network.

Bash Command 1: Deploy Blockchain Network (Hyperledger Fabric)

```
1.  //generate configuration
2.  cryptogen generate --config=./crypto-config.yaml
3.  //generate genesis block
4.  configtxgen -profile OneOrgOrdererGenesis -outputBlock ./config/genesis.block
5.  // Blockchain initialize
6.   docker-compose up -d
7.  // Generate genesis transaction
8.  configtxgen -profile TwoOrgChannel -outputCreateChannelTx ./config/assetschannel.tx -channelID
    assetschannel
9.  // Create the channel
10. docker exec cli peer channel create -o orderer.medicalblockchain.com:7050 -c assetschannel -f
    /etc/hyperledger/config/assetschannel.tx
11. // node join the channel
12. docker exec cli peer channel join -b assetschannel.block
```

After entering these commands, the preparation work is done and the blockchain network is running as below figure.

```
Creating network "deploy_default" with the default driver
Creating orderer.medicalblockchain.com ... done
Creating cli                           ... done
Creating peer0.org0.medicalblockchain.com ... done
Creating peer0.org2.medicalblockchain.com ... done
Creating peer1.org1.medicalblockchain.com ... done
Creating peer1.org0.medicalblockchain.com ... done
Creating peer1.org2.medicalblockchain.com ... done
Creating peer0.org1.medicalblockchain.com ... done
```

Figure 19: Terminal content when starting a blockchain network

The next step is deploying our chain code in the channel. The detailed chain code deployment process is shown in the diagram below:

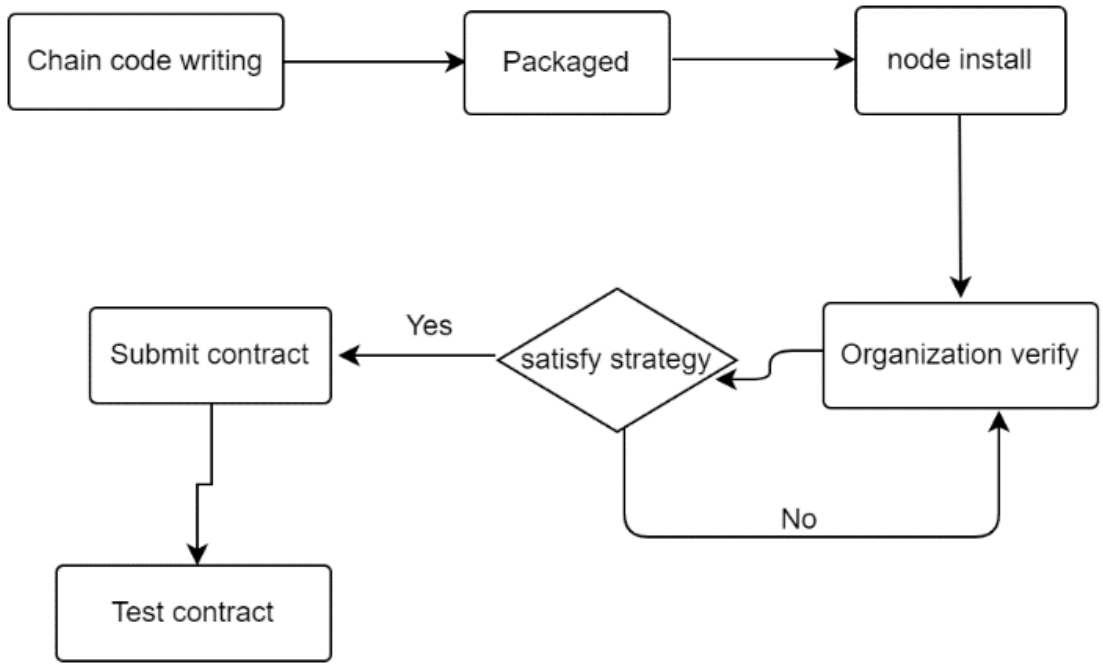


Figure 20: Chain code deployment process of chain code in Fabric 2.0

And here are bash commands to install our chain code in the channel and test it.

Bash Command 2: Deploy Smart Contract on the channel (Hyperledger Fabric)

1. //install the chain code
2. docker exec cli peer chaincode install -n blockchain_medical -v 1.0.0 -l golang -p /chaincode/blockchain-medical
3. //Instantiation of chain code
4. docker exec cli peer chaincode instantiate -o orderer.medicalblockchain.com:7050 -C assetschannel -n blockchain-medical -l golang -v 1.0.0 -c '{"Args":["init"]}')
5. // test chain code
6. docker exec cli peer chaincode invoke -C assetschannel -n blockchain-medical -c '{"Args":["queryAccountList"]}'

After the firstly deployment of the blockchain network in a single host, we transplanted it to Linux computers in the laboratory. We succeeded to deploy the multiple host blockchain environment and finished the simple data transfer between two computers.

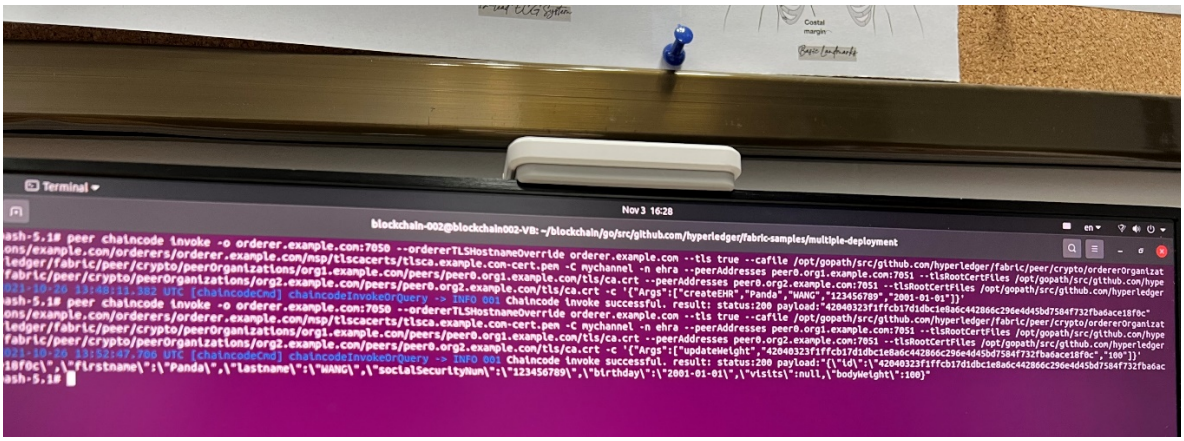


Figure 21: Finished a bodyweight data transfer between two machines in the laboratory

5.4 Smart Contract Implementation

According to the functionalities in design, the smart contract needs to automatically complete the health report uploading from the data exchange center and querying from medical institutions. Here is the class diagram that shows the interactions between modules.

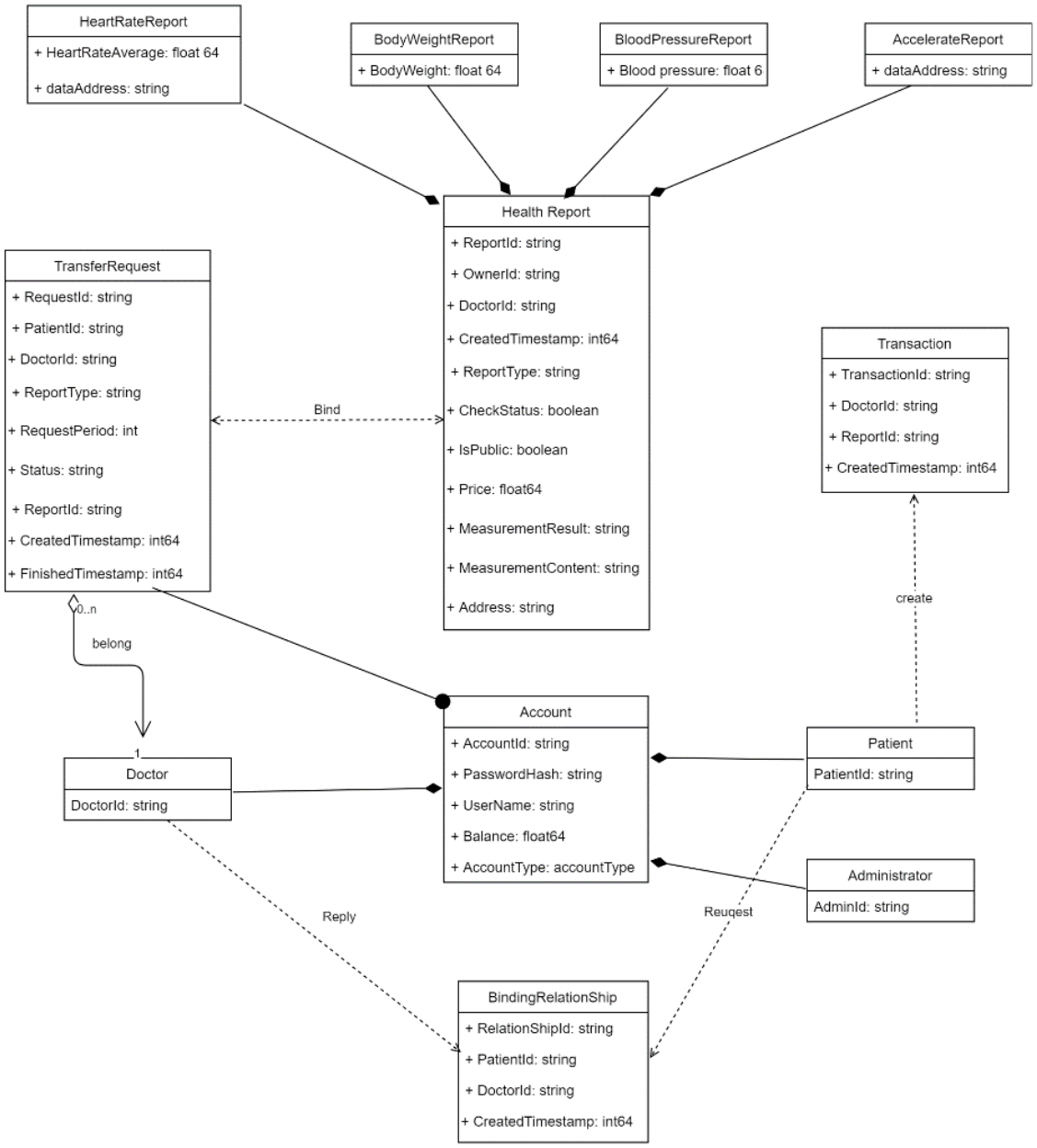


Figure 22: Class diagram of medical data sharing system

Then we implement the smart contract in chain code. There are two kinds of data structures that will be uploaded on the blockchain: health report, account, and report access record. The health report is the kernel on-chain information. It includes a unique report ID, the owner's ID (Patient's Public Key), doctor's ID (Doctor's public key), created time, report type, status (if the report has been accessed and if the report is set to be public), price (function not implemented, expandable for future work), measurement results and the address of report in data exchange centre. The pseudocode of the report data structure on-chain is as below:

Data structure 1: Transaction

```
type MedicalReport struct {
        ReportId          string  `json:"reportId"`
        OwnerId           string  `json:"ownerId"`
        DoctorId          string  `json:"ownerId"`
        CreatedTimestamp  int64   `json:"createdTimestamp"`
        ReportType        string  `json:"ReportType"`
        CheckStatus       bool    `json:"checkStatus"`
        IsPublic          bool    `json:"isPublic"`
        Price             float64 `json:"price"`
        MeassurementResult string  `json:"meassurementResult"`
        MeasureContent    string  `json:"measureContent"`
        Address           string  `json:"address"`
}
```

After defining the data structures that will be written on the distributed ledger, there are two kernel functions defined in the chain code: health report uploading and report querying. According to the system design, patients in the smart health home could not access the blockchain directly. Instead of it, the data exchange center will access the blockchain and upload the report for proxy. The uploading function needs seven inputs: patient public key, doctor public key, report type, price* (not necessary, just expandable for future), measurement result (for some simple measurements), content, address in the data exchange centre database and the hash value of the patient private key (to validate if the owner's identification is true). And then the smart contract will create a reported asset in the blockchain and insert the state database with the report key.

```
func CreateMedicalReport(stub shim.ChaincodeStubInterface, args []string) pb.Response {
    if len(args) != 7 {
        return shim.Error("Not correct parameter")
    }
    ownerId := args[0]
    doctorId := args[1]
    reportType := args[2]
    price := args[3]
    result := args[4]
    content := args[5]
    address := args[6]
    password := args[7]
    if ownerId == "" || doctorId == "" || reportType == "" || price == "" || result == "" || content == "" || address == "" {
        return shim.Error("empty par")
    }
.........
if err := WriteLedger(report, stub, ReportKey, []string{report.DoctorId, report.ReportId}); err != nil {
    return shim.Error(fmt.Sprintf("%s", err))
}

reportByte, err := json.Marshal(report)
if err != nil {
    return shim.Error(fmt.Sprintf("Error: %s", err))
}

return shim.Success(reportByte)
```

Figure 23: create Medical Report function in chain code

Another kernel function in chain code is querying health reports. According to the designed system, the doctor could query the patient's health report with the patient's public key (for targeted search) and his private key (for identification validation). Doctors access the blockchain from the node in the medical institutions.

```
func QueryReportList(stub shim.ChaincodeStubInterface, args []string) pb.Response {
    if len(args) != 2 {
        return shim.Error("para error")
    }
    reportId := args[0]
    doctorId := args[1]

    var reportList []MedicalReport
    results, err := GetStateByPartialCompositeKeys(stub, ReportKey, []string{doctorId, reportId})
    if err != nil || len(results) != 1 {
        return shim.Error(fmt.Sprintf("%s", err))
    }
    for _, v := range results {
        if v != nil {
            var report MedicalReport
            err := json.Unmarshal(v, &report)
            if err != nil || report.DoctorId != doctorId {
                return shim.Error(fmt.Sprintf("QueryReportList-error: %s", err))
            }
            reportList = append(reportList, report)
        }
    }
    reportListByte, err := json.Marshal(reportList)
    if err != nil {
        return shim.Error(fmt.Sprintf("QueryReportList-error: %s", err))
    }
```

Figure 24: query Medical Report function in chain code

5.5 Backend Implementation

The backend provides the ability to deal with blockchain access requests. According to the design, the backend server should be deployed in the data exchange center. After receiving the requests, the backend will parse the parameters that are transferred and execute the chain code invoke the function. The backend encapsulates the Application Programming Interfaces (APIs) and provides them to the front end. Then the user could send the requests to the backend by Website. Here is an example of the backend function of the query report below.

```go
func QueryReport(c *gin.Context) {
    appG := app.Gin{C: c}
    body := new(ReportQueryRequestBody)
    //parse body
    if err := c.ShouldBind(body); err != nil {
        appG.Response(http.StatusBadRequest, "error", fmt.Sprintf("para error%s", err.Error()))
        return
    }
    var bodyBytes [][]byte

    if body.ReportId != "" {
        bodyBytes = append(bodyBytes, []byte(body.ReportId))
        bodyBytes = append(bodyBytes, []byte(body.DoctorId))
    }

    //call smart contract
    resp, err := bc.ChannelQuery("queryReport", bodyBytes)
    if err != nil {
        appG.Response(http.StatusInternalServerError, "defeat", err.Error())
        return
    }
    // deserialized json
    var data []map[string]interface{}
    if err = json.Unmarshal(bytes.NewBuffer(resp.Payload).Bytes(), &data); err != nil {
        appG.Response(http.StatusInternalServerError, "error", err.Error())
        return
    }
    appG.Response(http.StatusOK, "sccuess", data)
}
```

Figure 25: query Medical Report function in the backend

5.6 User Interface

There are three types of accounts that could enter the website: administrator, patient, and doctor. The patient account represents the users in the smart health home. The doctor account represents users in medical institutions and the administrator account represents the data exchange center. Only the administrator could upload the health report.

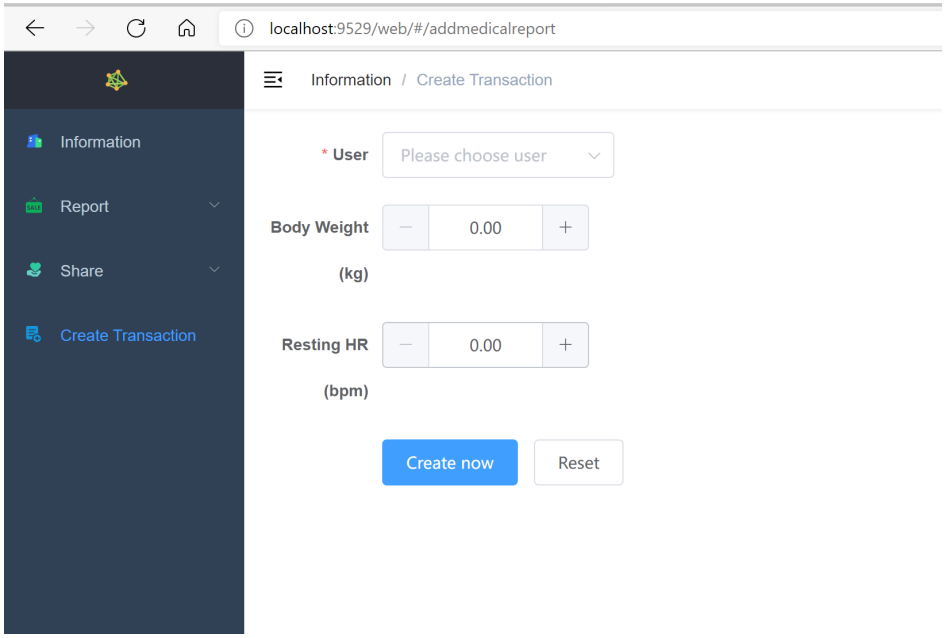


Figure 26: Create a report page

After the health report is uploaded on-chain, the patient user could see the information of the report. Users could choose a doctor to send this report to or share this report. If the health report is shared. All the medical institutions on the chain could view it and download it.

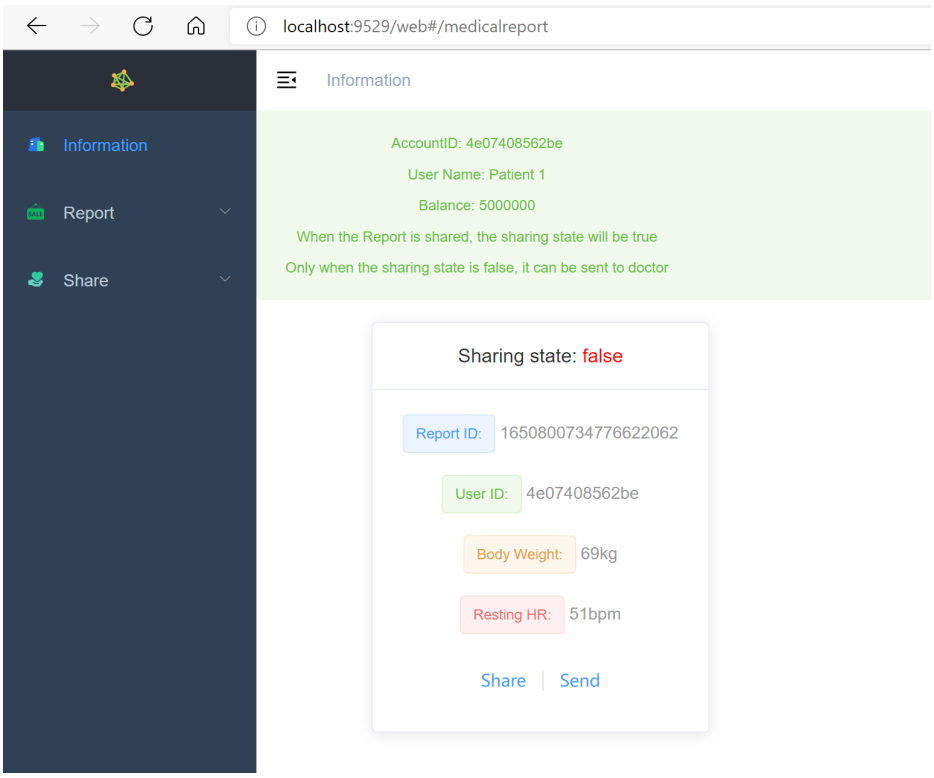


Figure 27: Report home page for patient users

When the user with a doctor account enters the website, he will see the unconfirmed report and can confirm to receive it. After confirming, the doctor could get the address and validation key of this report. Using these two things, the doctor can query the complete health report. Because we cannot develop a real DEC, we must store simple data on the blockchain and get it directly.

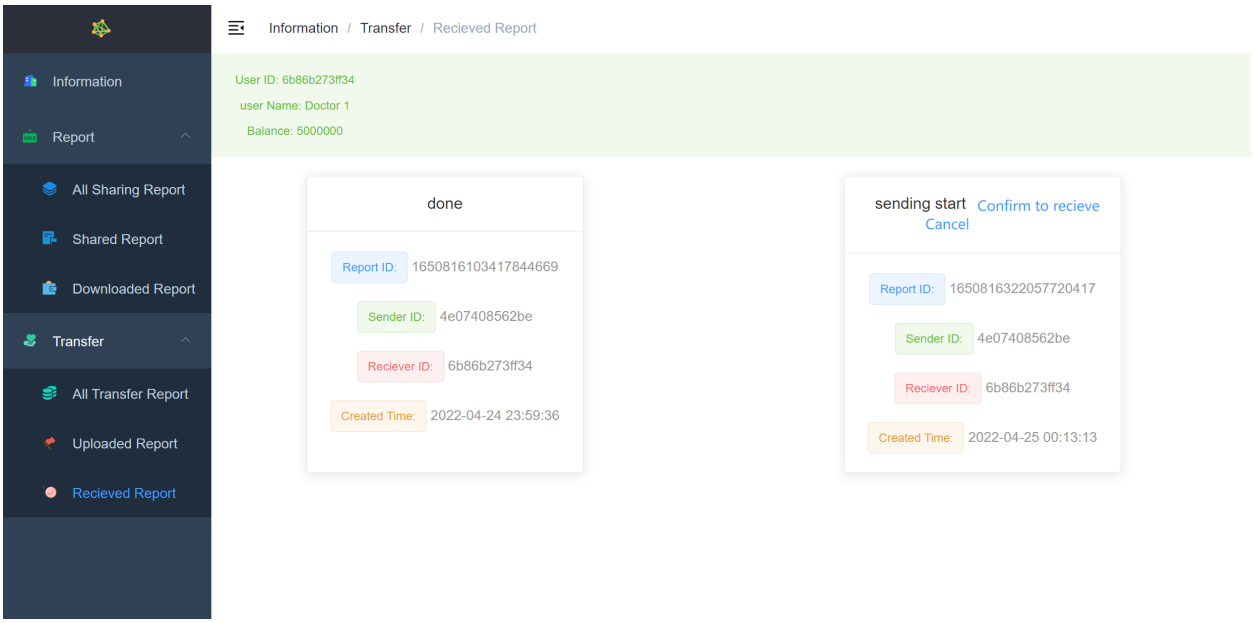


Figure 28: report confirming page for doctor account

Users with a doctor account could also access all the public health reports. As soon as the report becomes publicly available, the user could not undo this action. We designed a credit system for downloading public reports but did not implement it. The APIs are reserved for future work.

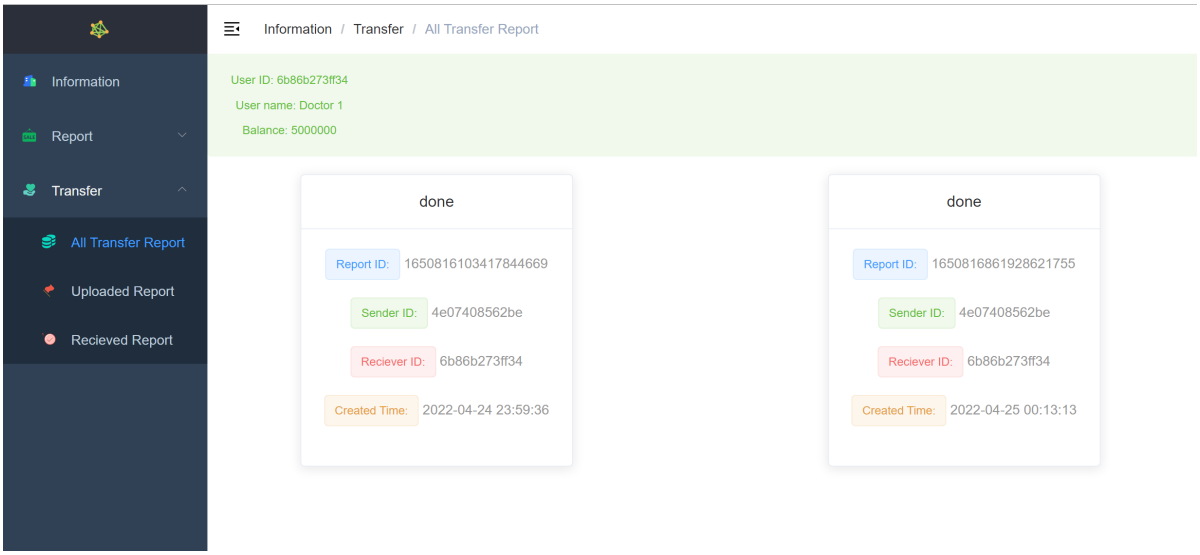


Figure 29: sharing report page for doctor

6 Summary

6.1 Conclusion

The main contribution of this project is that we design, implement, and test a blockchain-based SHH system for medical data management and sharing between nodes: Smart Health Home, data exchange center, and health care institution. This medical blockchain system provides a trusted environment between SHH and hospitals for improved health care delivery. We finished the blockchain network deployment between multiple osts, and developed a smart contract for multiple data transfers, and a website for users to finish data sharing. Overall, the project shows its big potential in the new field: blockchain for medical data transfer between SHH and health care institutions. It could be very helpful for long term diagnosis and provide a convenient solution to medical data sharing between institutions when more hospitals join the medical blockchain alliance in the future.

6.2 Future Work

Further studies will focus on data exchange center implementation and expanding medical transfer protocols. In addition, the report generated from the smart health home could be uploaded automatically, which means moving forward a step on confirming the validation of data. Another interesting aspect, the credit system could be added if we could find a suitable mechanism. A credit system or token module can inspire the patient to share their data for medical research and charge fee from medical institutions for blockchain maintenance. This function should be considered very carefully because it means cryptocurrencies are directly tied to real money and a series of troubles might come.

7 Evaluation

7.1 Reflection

This medical blockchain project started during summer holidays last year. I joined Prof. Brusic's summer research group and learnt knowledge in the medical blockchain area. And we had the initial understanding of doing research and designing the system. Then I came to wanxiang blockchain company for a summer internship and to study more blockchain projects. In the first semester, we finished the literature review about blockchain technology, the applications of blockchain in the field of the storage system and medical systems. Then we came up with the preliminary design of the whole system structure, interaction procedure between different actors, possible encryption method and blood pressure measurement protocol as the case study. In the second semester, I finished the development of the final smart contract, backend, and website (front end) of this project with Jiawei, who has a financial blockchain project and the same supervisor as me.

The project started by proposing ten key objectives (see Aims and Objectives Section). The design of the medical blockchain system has been finished and the procedure of making a transaction for medical report transfer has been ensured. Almost all the design work is finished on schedule while implementation of blockchain took a longer time than expected. The case study of medical data transfer protocol only includes blood pressure and body weight. In that case, more medical data report protocols need to be designed in the future. Compared with the initial project plan, the results are not bad, and I have finished the implementation work. My programming skills need to be strengthened so that I could save more time on implementation. While the current system is not a complete medical blockchain system, the DEC is still simulated. The research aspect is the weak point until now. I need to spend more time learning these successful designs of blockchain systems and consider more realistic factors.

7.2 Project Schedule and Deliverables

The Project Plan activities, deliverables, and their schedule are presented in the Gantt chart (Tables 15). The project activities include:

A. Administrative
    1. Prepare project proposal. The deliverable – project proposal document
    2. Complete the ethics checklist. Deliverable – ethics checklist (no ethics approval will be sought)

3. Perform presentation and submission of required deliverables as scheduled. Deliverable – as scheduled.

B. Design
   1. The medical blockchain system structures
   2. Encryption Method to ensure the privacy and security
   3. Credit system (Advanced function)

C. Implementation
   1. Single host multi-nodes blockchain network deployment
   2. Medical Blockchain System (Back-end client and Front-end client)
   3. Smart Contract (Allow user to upload and download data, send, or reply to a binding request)
   4. Encryption system

D. Testing
   1. Blockchain network test
   2. System test
   3. Smart contract test
   4. Encryption test

E. Reporting
   1. Interim Report writing. Deliverable – interim report.
   2. Dissertation writing. Deliverable – dissertation

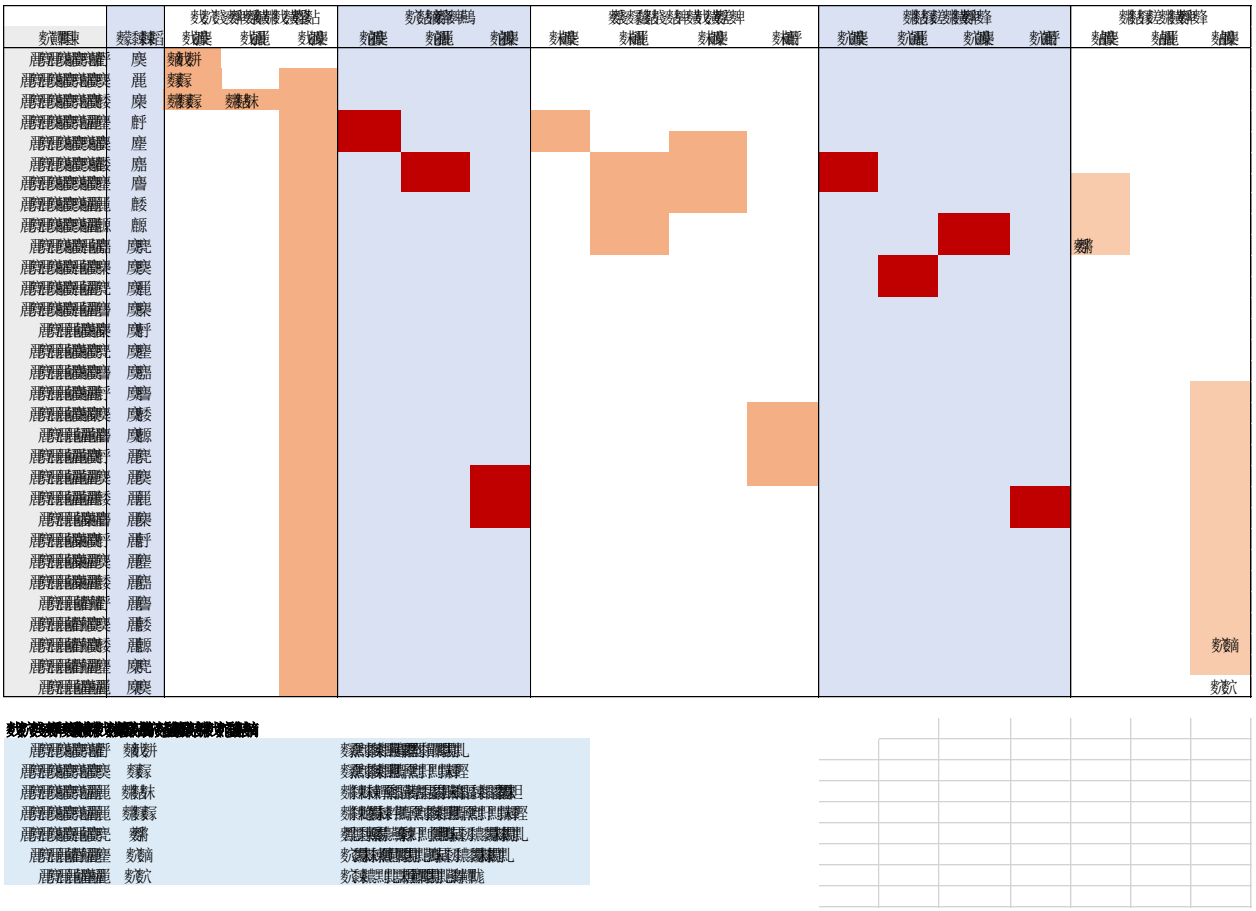


Table 5: Initial Gantt Chart of this project

Date	Week	ADMINISTRATIVE A.1	A.2	A.3	DESIGN B.1	B.2	B.3	IMPLEMENTATION C.1	C.2	C.3	REPORTING D.1	D.2	D.3	REPORTING E.1	E.2	E.3
2021/10/4	1	SAF														
2021/10/11	2	PP														
2021/10/18	3	RPP	REC													
2021/10/25	4															
2021/11/1	5															
2021/11/8	6															
2021/11/15	7															
2021/11/22	8															
2021/11/29	9															
2021/12/6	10													IR		
2021/12/13	11															
2021/12/20	12															
2021/12/27	13															
2022/1/3	14															
2022/1/10	15															
2022/1/17	16															
2022/1/24	17															
2022/1/31	18															
2022/2/7	19															
2022/2/14	20															
2022/2/21	21															
2022/2/28	22															
2022/3/7	23															
2022/3/14	24															
2022/3/21	25															
2022/3/28	26															
2022/4/4	27															
2022/4/11	28															
2022/4/18	29															DS
2022/4/25	30															
2022/5/2	31															DD

Table 6: Final Gantt Chart of this project

Bibliography

[1] M. Chan, D. Estève, C. Escriba, and E. Campo, “A review of smart homes—Present state and future challenges,” *Computer Methods and Programs in Biomedicine,* vol. 91, no. 1, pp. 55-81, 2008/07/01/, 2008.

[2] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, “Blockchain,” *Business & Information Systems Engineering,* vol. 59, no. 3, pp. 183-187, 2017.

[3] C. S. Wright, “Bitcoin: A peer-to-peer electronic cash system,” *Available at SSRN 3440802*, 2008.

[4] L. Yu, W. Xie, D. Xie, Y. Zou, D. Zhang, Z. Sun, L. Zhang, Y. Zhang, and T. Jiang, “Deep Reinforcement Learning for Smart Home Energy Management,” *IEEE Internet of Things Journal,* vol. 7, no. 4, pp. 2751-2762, 2020.

[5] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management."

[6] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, “MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain,” *Journal of Medical Systems,* vol. 42, no. 8, 2018.

[7] A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B.-G. Kim, “Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare,” *Electronics,* vol. 9, no. 10, pp. 1609, 2020.

[8] M. A.-U.-D. Khan, M. F. Uddin, and N. Gupta, "Seven V's of Big Data understanding Big Data to extract value."

[9] X. Zhang, J. Zhang, M. Pike, N. M. Mustafa, D. Towey, and V. Brusic, "Sensor Networks and Personal Health Data Management: Software Engineering Challenges," pp. 140-159: Springer International Publishing, 2021.

[10] L. M. S. D. Nascimento, L. V. Bonfati, M. L. B. Freitas, J. J. A. Mendes Junior, H. V. Siqueira, and S. L. Stevan, “Sensors and Systems for Physical Rehabilitation and Health Monitoring—A Review,” *Sensors,* vol. 20, no. 15, pp. 4063, 2020.

[11] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” *Future Generation Computer Systems,* vol. 107, pp. 841-853, 2020.

[12] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data."

[13] IBM. "Blockchain overview," https://www.ibm.com/topics/what-is-blockchain.

[14] S. S. Gupta, “Blockchain,” *IBM Onlone (http://www. IBM. COM)*, 2017.

[15] D. Yaga, P. Mell, N. Roby, and K. Scarfone, *Blockchain technology overview*, National Institute of Standards and Technology, 2018.

[16] M. Pilkington, "Blockchain technology: principles and applications," *Research handbook on digital transformations*: Edward Elgar Publishing, 2016.

[17] R. Banger, “A Study On BlockChain And Cryptography,” *Journal of Emerging Technologies and Innovative Research*, 2019.

[18] R. Rivest, *The MD5 message-digest algorithm,* 2070-1721, 1992.

[19] D. Eastlake 3rd, and P. Jones, *US secure hash algorithm 1 (SHA1),* 2070-1721, 2001.

[20] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption." pp. 394-403.

[21] K. Lauter, “The advantages of elliptic curve cryptography for wireless security,” *IEEE Wireless communications,* vol. 11, no. 1, pp. 62-67, 2004.

[22] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang, “Digital signature scheme for information non-repudiation in blockchain: a state of the art review,” *EURASIP Journal on Wireless Communications and Networking,* vol. 2020, no. 1, 2020.

[23] L. Zhou, L. Wang, and Y. Sun, “MIStore: a Blockchain-Based Medical Insurance Storage System,” *Journal of Medical Systems,* vol. 42, no. 8, 2018.

[24] S. Wang, Y. Zhang, and Y. Zhang, “A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems,” *IEEE Access,* vol. 6, pp. 38437-38450, 2018.

[25] J. Benet, and N. Greco, “Filecoin: A decentralized storage network,” *Protoc. Labs*, pp. 1-36, 2018.
[26] E. Nyaletey, R. M. Parizi, Q. Zhang, and K.-K. R. Choo, "BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability."
[27] M. Ali, J. Nelson, R. Shea, and M. J. Freedman, "Blockstack: A global naming and storage system secured by blockchains." pp. 181-194.
[28] E. R. Ritenour, “Hacking and ransomware: challenges for institutions both large and small,” *American Journal of Roentgenology,* vol. 214, no. 4, pp. 736-737, 2020.
[29] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, and D. S. Wong, “Designing cloud-based electronic health record system with attribute-based encryption,” *Multimedia Tools and Applications,* vol. 74, no. 10, pp. 3441-3458, 2015.
[30] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, “Blockchain-based medical records secure storage and medical service framework,” *Journal of medical systems,* vol. 43, no. 1, pp. 1-9, 2019.
[31] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain." p. 650.
[32] 梅颖, “安全存储医疗记录的区块链方法研究,” *江西师范大学学报: 自然科学版*, no. 5, pp. 484-490, 2017.
[33] I. Sommerville, “Software engineering,” 1994.
[34] J. Hunt, “Feature-driven development,” *Agile Software Construction*, pp. 161-182, 2006.
[35] B. Kitchenham, and S. Charters, “Guidelines for performing systematic literature reviews in software engineering,” 2007.
[36] I. Sommerville, *Requirements Engineering*, 9 ed., p.^pp. 82–118: Pearson, 2016.
[37] N. Szabo, “Formalizing and securing relationships on public networks,” *First monday*, 1997.
[38] M. Valenta, and P. Sandner, “Comparison of ethereum, hyperledger fabric and corda,” *Frankfurt School Blockchain Center,* vol. 8, pp. 1-8, 2017.
[39] H. Gilbert, and H. Handschuh, "Security analysis of SHA-256 and sisters." pp. 175-193.
[40] Y. S. Lee, E. Alasaarela, and H. Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system." pp. 453-457.
[41] P. Mahajan, and A. Sachdeva, “A study of encryption algorithms AES, DES and RSA for security,” *Global Journal of Computer Science and Technology*, 2013.
[42] X. Zhou, and X. Tang, "Research and implementation of RSA algorithm for encryption and decryption." pp. 1118-1121.
[43] J. Liu, “Highlights of the 2018 Chinese hypertension guidelines,” *Clinical hypertension,* vol. 26, no. 1, pp. 1-6, 2020.
[44] E. O'Brien, N. Atkins, G. Stergiou, N. Karpettas, G. Parati, R. Asmar, Y. Imai, J. Wang, T. Mengden, and A. Shennan, “European Society of Hypertension International Protocol revision 2010 for the validation of blood pressure measuring devices in adults,” *Blood pressure monitoring,* vol. 15, no. 1, pp. 23-38, 2010.
[45] P. G. Kopelman, “Obesity as a medical problem,” *Nature,* vol. 404, no. 6778, pp. 635-643, 2000.
[46] N. R. Council, “Weight gain during pregnancy: reexamining the guidelines,” 2010.
[47] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric."
[48] G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” *Ethereum project yellow paper,* vol. 151, no. 2014, pp. 1-32, 2014.

Appendix

A. Activity Diagram of Medical Blockchain system

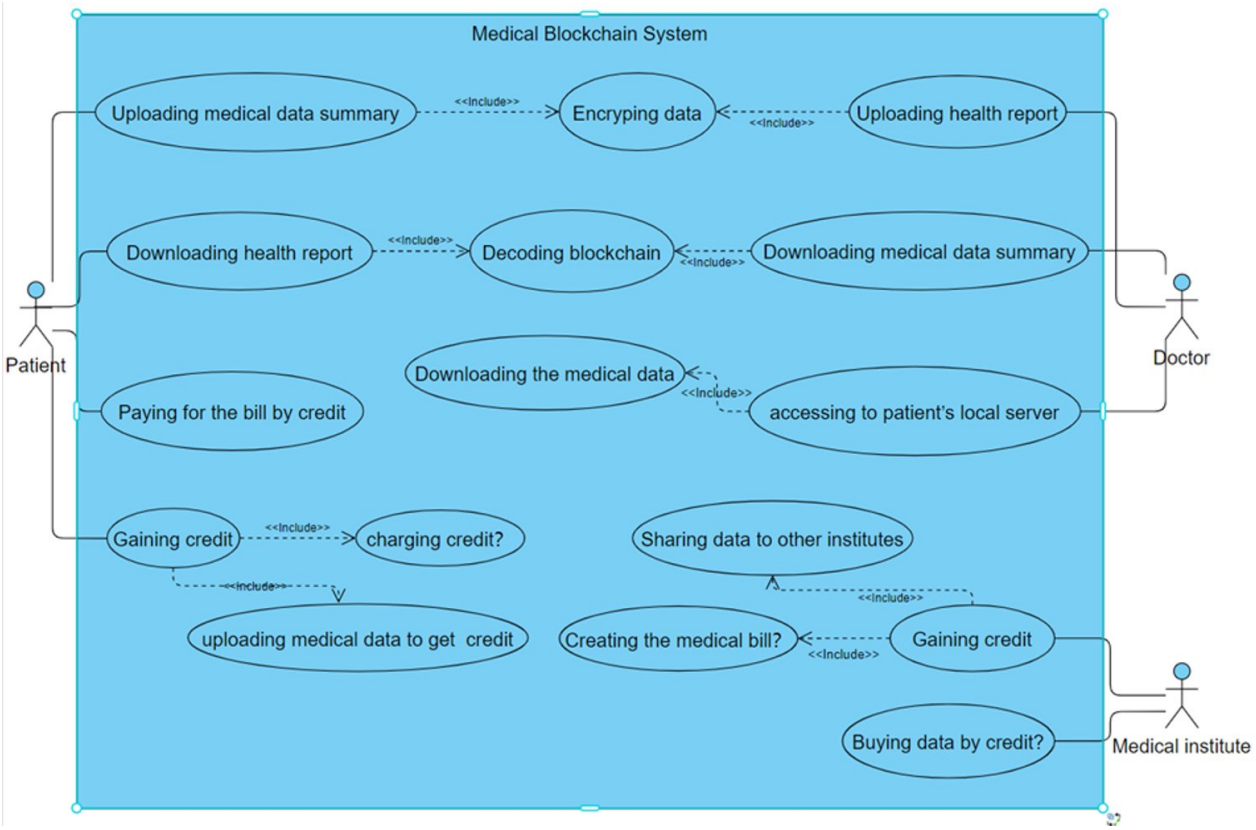


Figure 1: Activity diagram of the medical blockchain system

B. Network Architecture of Blockchain System in Smart Health Home

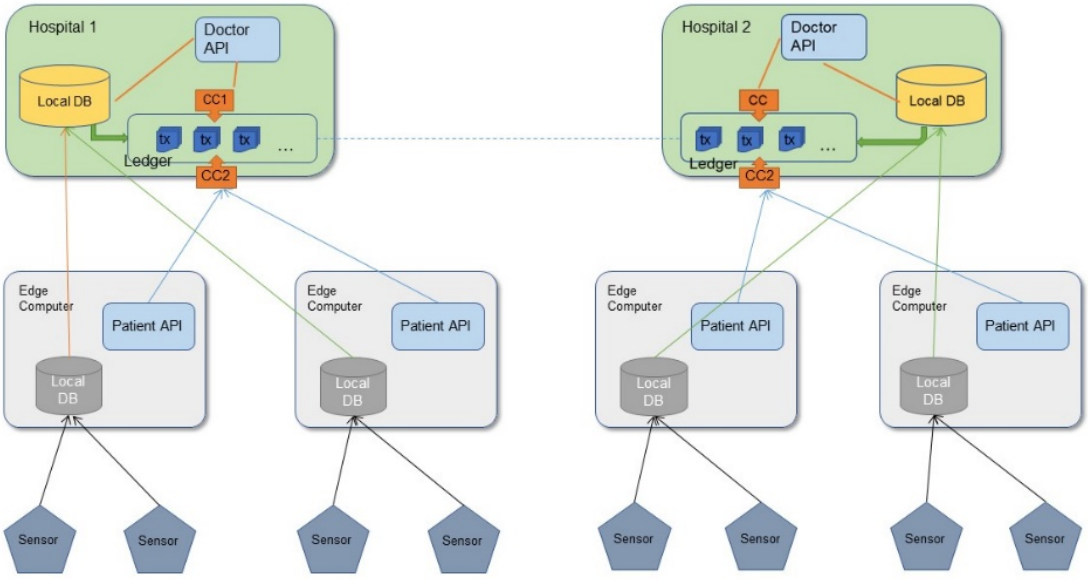


Figure 2：Network Architecture of Blockchain System in Smart Health Home

C. User Manual

1. Test Environment

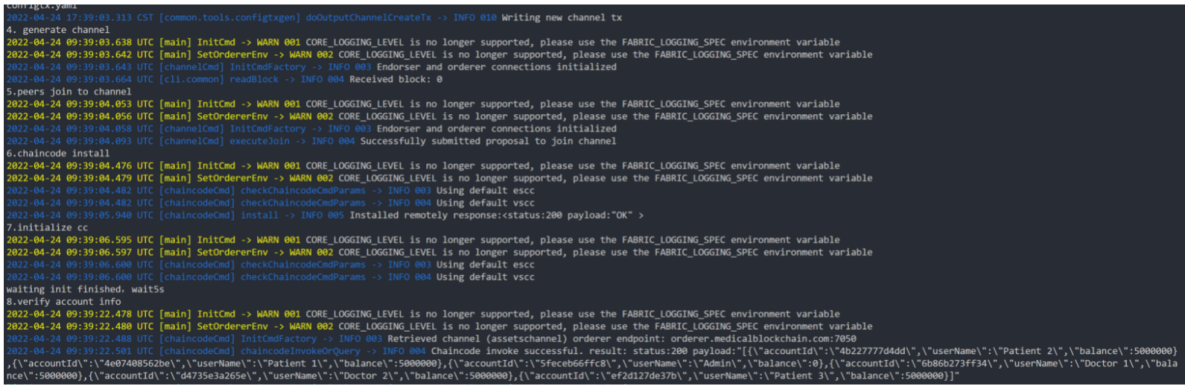
```
[root@localhost ~]# cat /etc/redhat-release
CentOS Linux release 7.9.2009 (Core)
[root@localhost ~]# docker -v
Docker version 20.10.6, build 370c289
[root@localhost ~]# docker-compose -v
docker-compose version 1.25.4, build 8d51620a
[root@localhost ~]#
```

2. Run the project

2.1. clone the project in the path：`/root/medical-blockchain`

2.2. give the project permission `sudo chmod -R +x /root/medical-blockchain/`

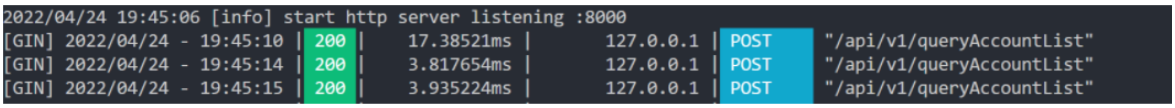
2.3. Enter `deploy` directory， excute `./start.sh` start blockchain network



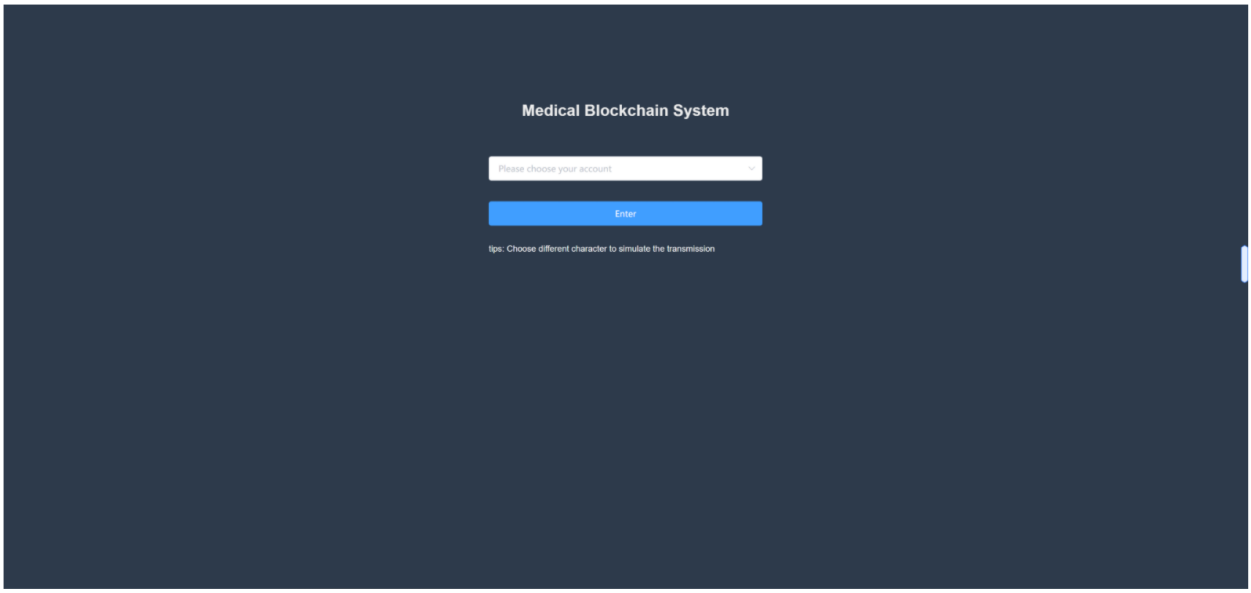
2.4 Enter `vue` directory， excute `./build.sh` compile front end

2.5 Enter `application` directory， excute `./build.sh` compile back end

2.6 In `application` directory， excute `./start.sh` start application

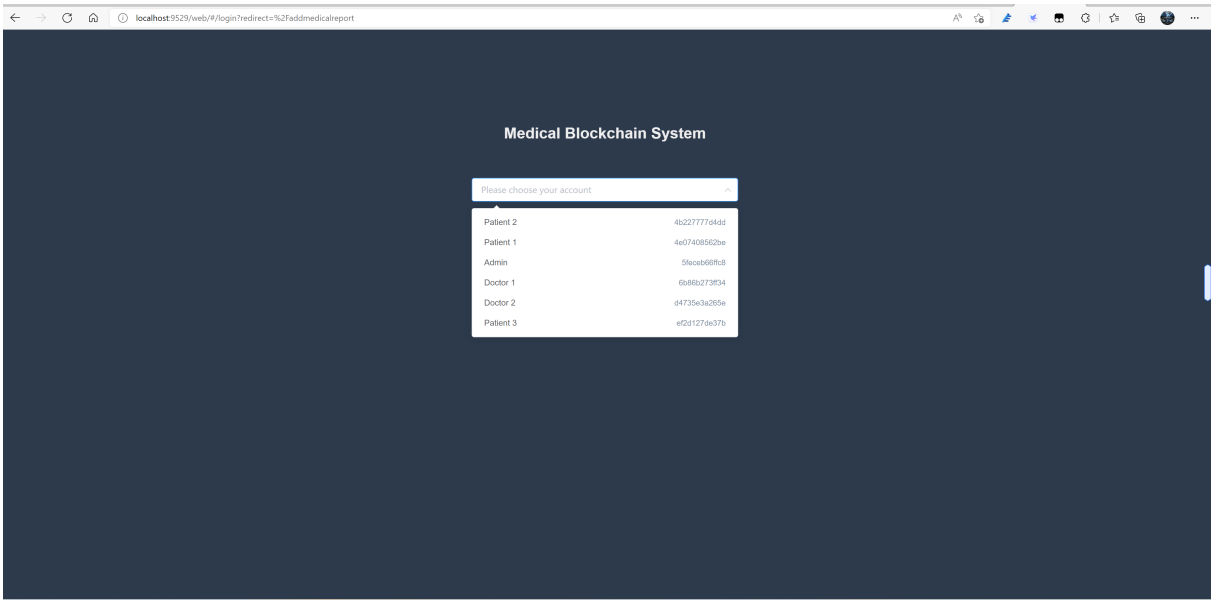


2.7 browser access http://localhost:8000/web

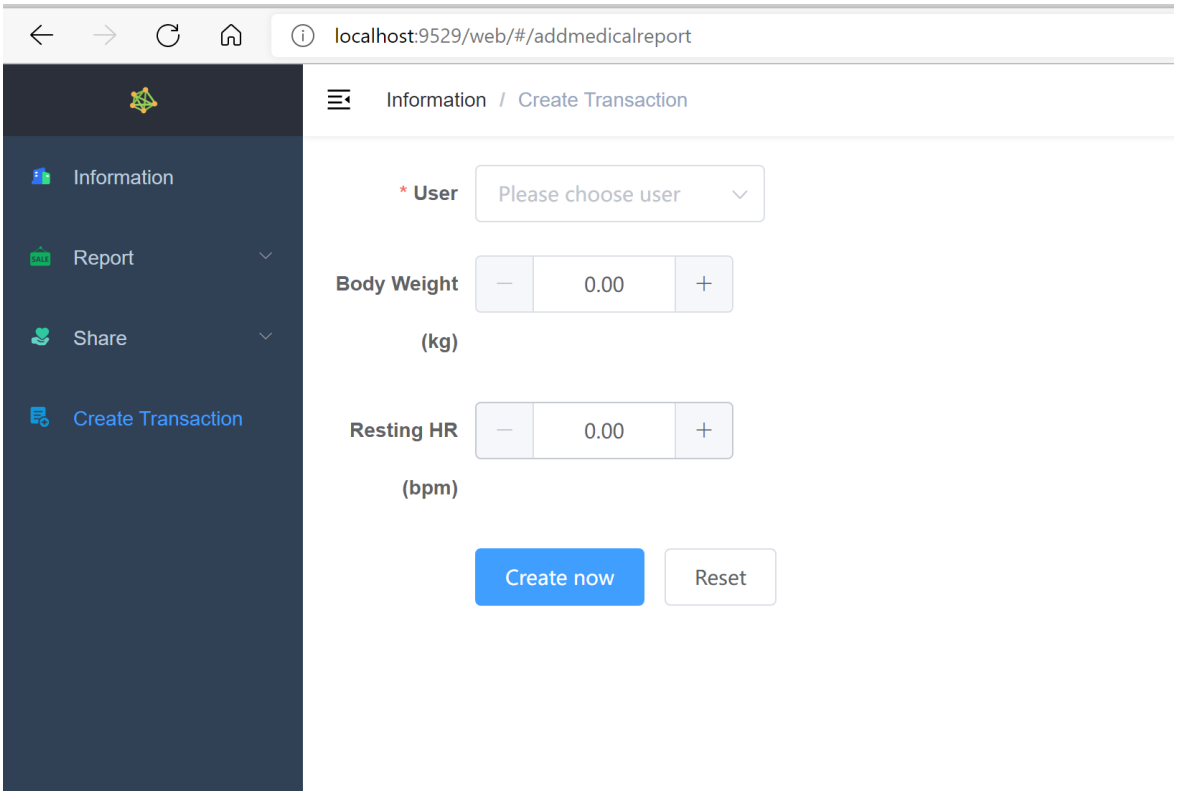


3. Login & Admin Page

choose an account to login the medical blockchain system

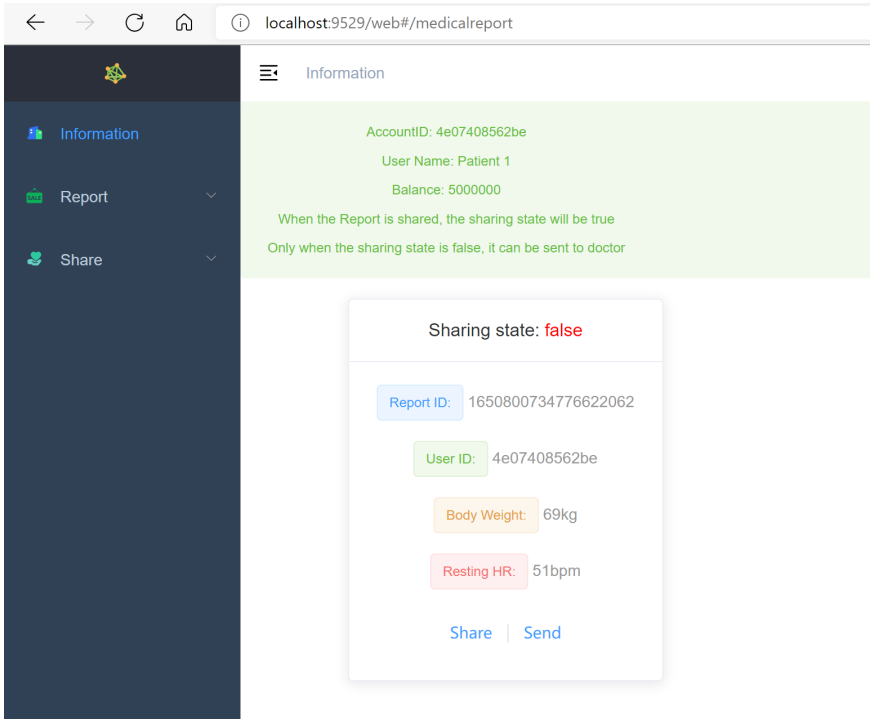


After login, user could see the account information and current reports that not sent

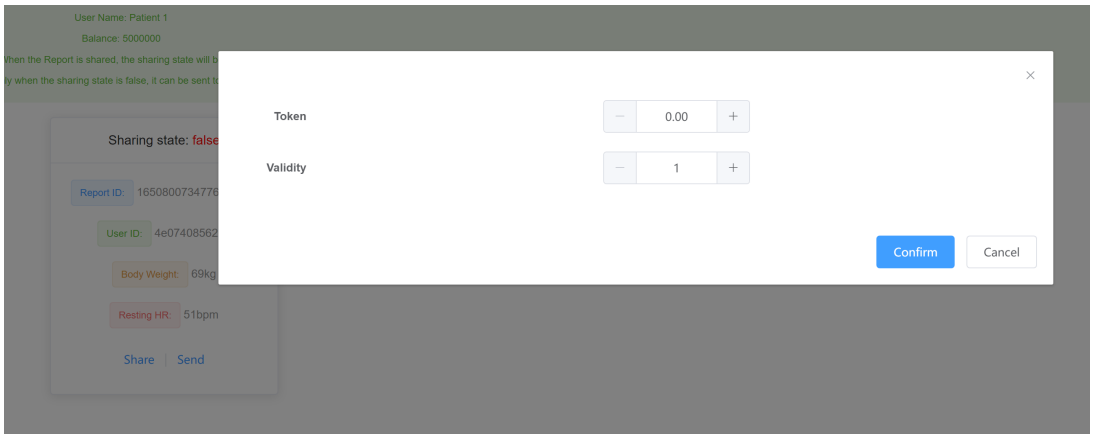


4. Patient Page

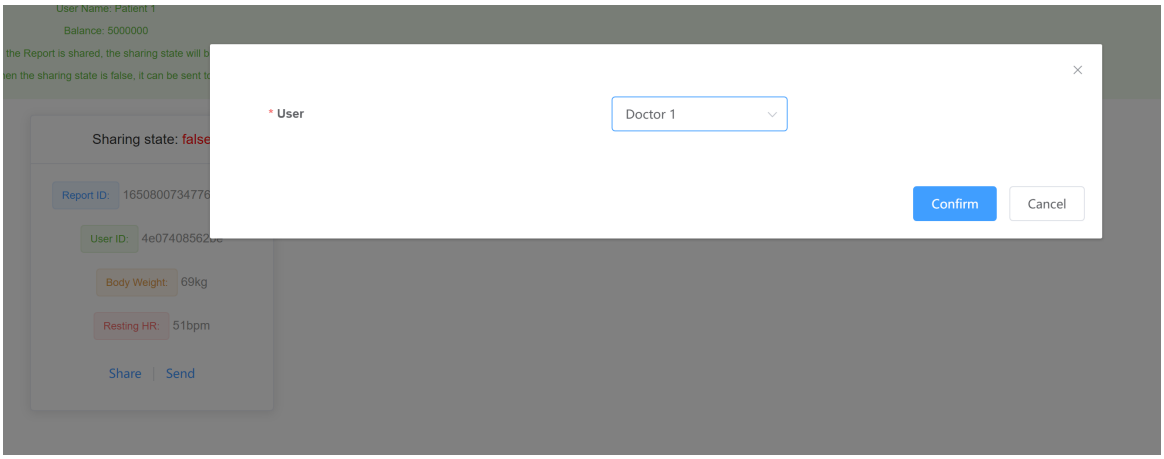
Patient could see his uploaded report and choose to send to doctor or share it.



Sharing report should set the token of it and its validity.

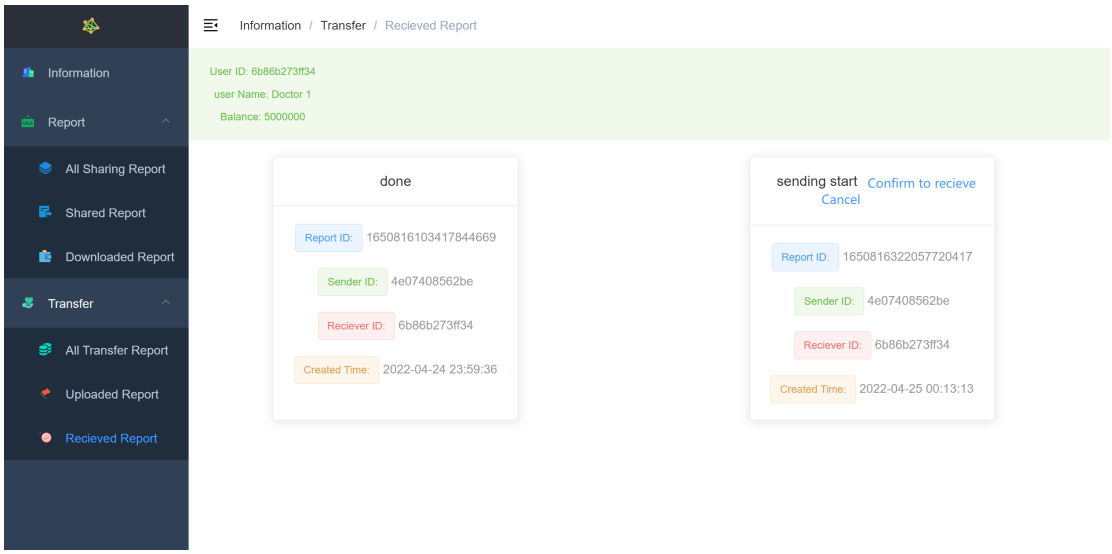


Sending report should choose the doctor.

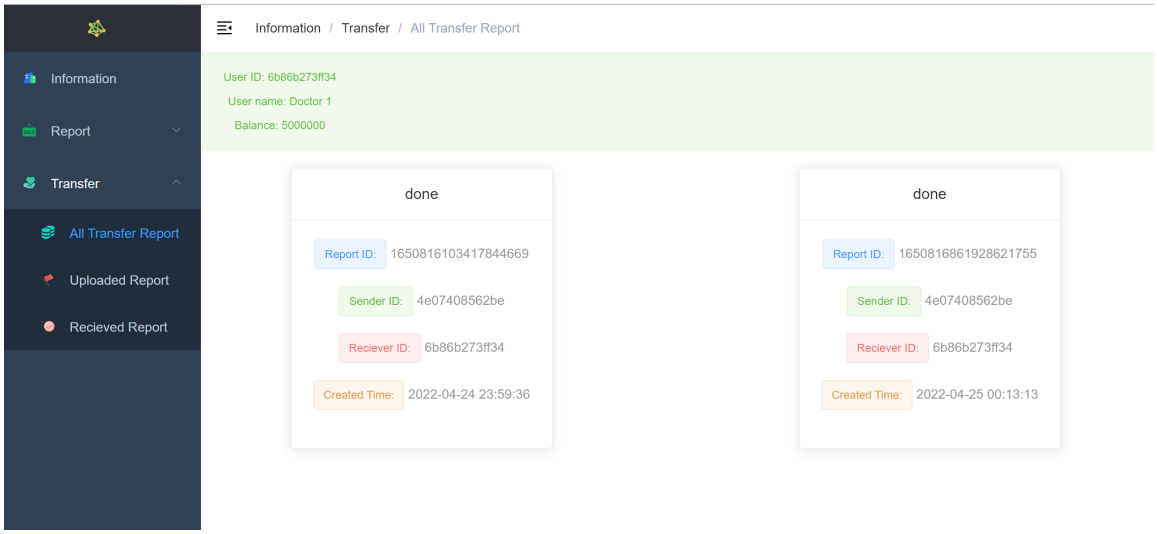


5. Doctor Page

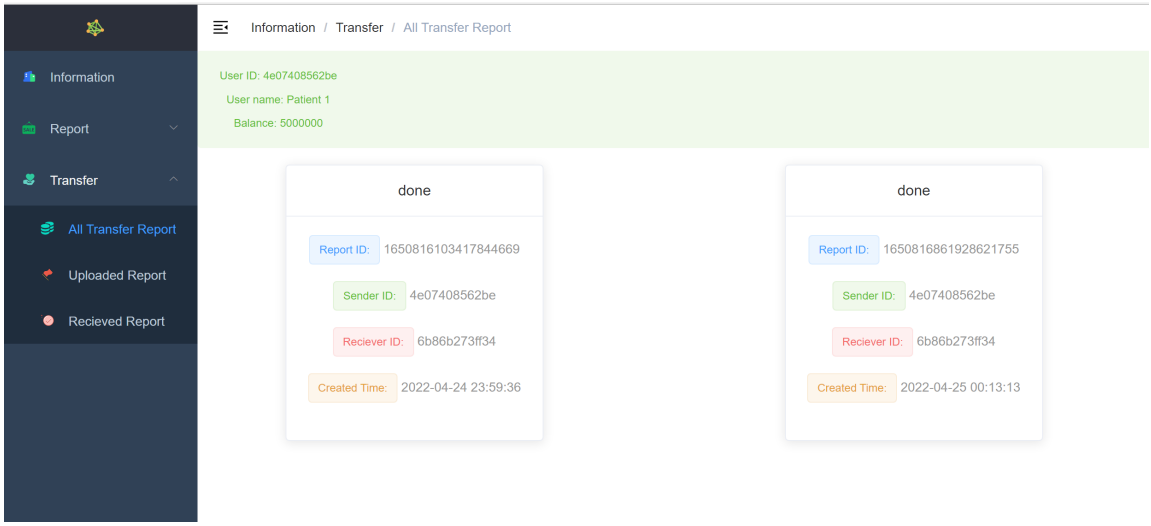
When doctor uses his account to login, he could see all shared health report



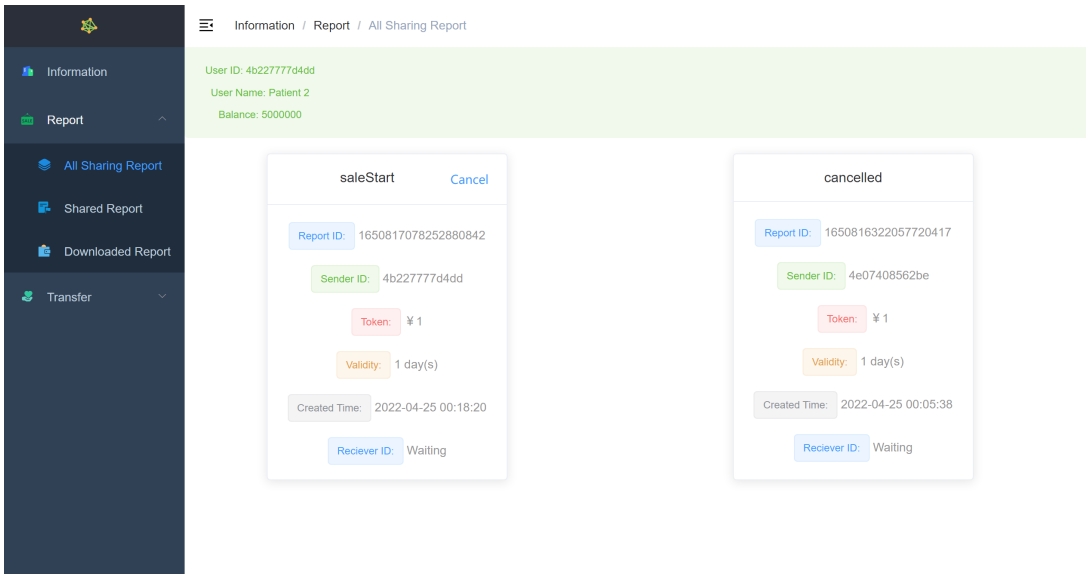
Then doctor could receive this report (downloaded data page).



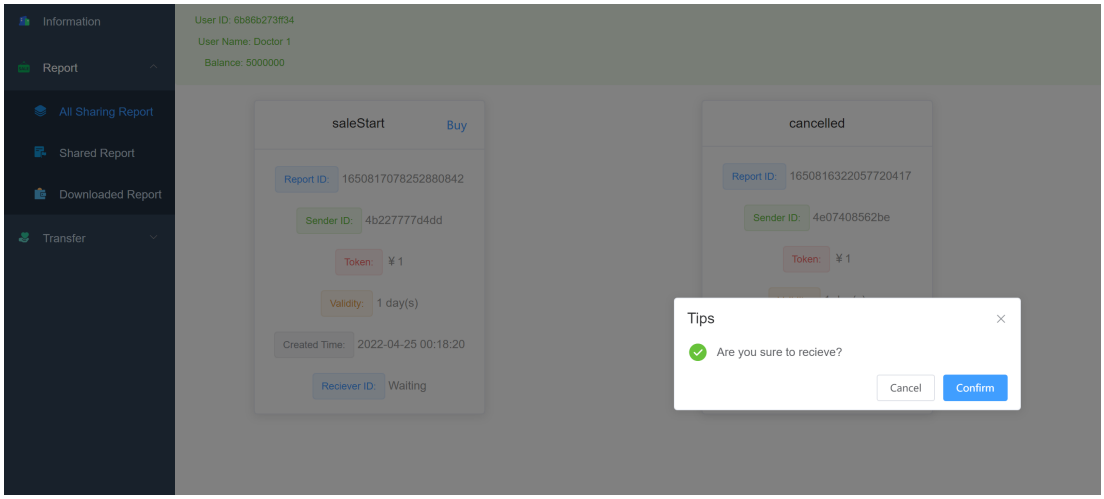
Then patient could also see the status of this transaction (uploaded data page)



After patient sharing a health report, it will be public, and all the medical institutions could see it.



They could pay some tokens to get the report.



Then the medical institution could see it in downloaded report page.