Computer and Systems Engineering Department
Faculty of Engineering
Alexandria University

Graduation Project Submitted In
Partial Fulfillment Of The B. SC. Degree

Blockchain-Based Health Care Data Manager

Authors:
Mohamed Tarek Aiad
Mohamed Mostafa Ibrahim
Ahmed Abdallah Abo-eleid
Mohamed Momen Salama
Michael Samir Azmy
Abdullatif Khalid Habiba

Supervisors:
Prof. Dr. Mohamed S. Abougabal
Prof. Dr. Shaimaa Lazem
Dr. Amira Elshazly
Dr. Samia Hafez

Acknowledgments

We extend our heartfelt gratitude to Allah for inspiring the inception of this project. Our deepest appreciation goes to Prof. Dr. Mohamed S. Abougabal, Prof. Dr. Shaimaa Lazem, and Dr. Amira Elshazly, not only for their roles as supervisors but also for their unwavering guidance, constant encouragement, and the challenges that propelled us to excel throughout the project. Their dedicated mentorship has been instrumental in ensuring the triumphant completion of this endeavor.

Our immense thanks also go to our families, whose boundless support has been a cornerstone of our success. Their enduring encouragement has been the driving force behind our achievements, making them an indispensable part of this journey. Without their love and care, our accomplishments would have been far from attainable.

Abstract

The confidentiality and security of healthcare records are pivotal for ensuring patient trust and the seamless delivery of healthcare services. Traditional healthcare record-keeping systems often face vulnerabilities related to unauthorized access, data breaches, and compromises in patient privacy. In response to these challenges, this project proposes a groundbreaking solution leveraging blockchain technology to revolutionize healthcare data management.

This research investigates the implementation of a secure and decentralized blockchain-based system designed specifically for storing and managing healthcare records. By utilizing the inherent cryptographic features and decentralized structure of blockchain, the project aims to establish an immutable and tamper-proof repository for storing sensitive patient information. This innovative approach not only ensures the integrity and security of healthcare data but also introduces a level of transparency and accountability essential in the healthcare domain.

Through an in-depth analysis of blockchain technology's application in healthcare, this project explores the potential benefits and challenges associated with migrating from conventional centralized healthcare databases to a distributed ledger-based framework.

The project's outcomes offer insights into the viability and feasibility of blockchain-based healthcare record systems, highlighting their potential to transform the healthcare landscape by fostering trust, enhancing security, and safeguarding patient confidentiality. This exploration serves as a significant contribution to the evolving discourse on utilizing cutting-edge technology to fortify data security and privacy in healthcare.

List of Figures

List of Tables

List of Acronyms

Term / Symbol	Meaning
PMR	Paper Medical Records
EMR	Electronic Medical Records
EHR	Electronic Health Records
HIE	Health Information Exchanges
PoW	Proof of Work
PoS	Proof of Stake
PoA	Proof of Authority
DPoS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
NFTs	Non-Fungible Tokens
EVM	Ethereum Virtual Machine
EOA	Externally Owned Account
CA	Certificate Authorities
HF	Hyperleger Fabric
Fabric CA	Fabric Certificate Authority
MSP	Membership Service Provider
HIPAA	Health Insurance Portability and Accountability Act
GDPR	General Data Protection Regulation
IPFS	InterPlanetary File System
API	Application Programming Interface
HLF	Hyperledger Fabric
UML	Unified Modeling Language

Contents

Chapter One

1 Introduction

1.1 General

The healthcare industry in Egypt has witnessed significant advancements through the integration of automation and digital transformation. Despite some countries successfully adopting a general medical insurance system to streamline medical data and enhance patient care, Egypt still grapples with traditional data transfer methods, such as sharing paper prescriptions, leading to a substantial data backlog.
In response to these challenges, our project aims to introduce a groundbreaking solution: a medical data manager utilizing blockchain technology to revolutionize the Egyptian healthcare system. Despite the numerous benefits of healthcare data, many patients in Egypt encounter obstacles in accessing timely and accurate medical health records. The reliance on traditional diagnostic methods and the cumbersome process of obtaining lab reports and scans impede the efficiency of healthcare services.
To address this gap, our project proposes the implementation of electronic health records (EHR) integrated with blockchain technology. Our medical data manager harnesses the power of blockchain to ensure secure, transparent, and immutable storage of medical data, thereby fostering trust among both patients and healthcare providers.

1.2 Motivation

There are certain diseases for which a uniform treatment that suits all patients with this ailment hasn't been discovered. However, they are treated through medication trials, observing their effects on patients, and gauging their response to this treatment. Based on this, the doctor decides whether the patient will continue with this medication or not. Examples of such diseases are cancer and skin diseases.

In Egypt, it is common for people to prefer visiting private clinics over going to hospitals, in addition to the fragmentation of the health system. For example, Cairo has only 134 government hospitals while it has more than 89 thousand private clinics [1]. This leads to inconsistencies in follow-ups, and it's common for individuals to consult multiple doctors in the same specialization for reassurance.

If a patient decides to consult another doctor for reassurance, several issues may arise. These include the patient forgetting the medications taken during the previous period, damaging or losing scans and tests, and necessitating their repetition.

Therefore, we decided to resort to recording all this data and transforming it from paper-based to digital. With the ongoing digital transformation by the government, this was a significant motivator for us.

Here lies the fundamental problem we aim to solve in our project: securely storing patients' health data while maintaining its privacy, ensuring that the patient is the only controller of the data to prevent any possible exploitation, such as threats or selling to companies and others.

Hence, we turned to the idea of blockchain, which we will elaborate on in detail in the upcoming discussions.

1.3 Organization of the report

The report is organized into four chapters.

First, in Chapter 1, we give a brief introduction and motivation.

In Chapter 2, an essential background and overview of health records and their development, blockchain and its types, like Ethereum and Hyperledger Fabric, and a quick explanation of Egyptian Data Law are provided.

In Chapter 3, related work and applications that tried to solve the problem are discussed. work needs to extend the scope of work.

Finally, Chapter 4 contains the platforms and tools we will use.

In the appendix, you can find a summary of some papers that we used to build our ideas.

Chapter Two

2 Background

2.1 Introduction

In chapter 1, a general description of the problem was presented and the motivation to develop our project.
In this chapter, a background about EHR is introduced from section 2.2 to section 2.4, a talk about why we could use blockchain technology with EHR is introduced in section 2.5, then some background about blockchain technology and blockchain networks is introduced from section 2.6 to section 2.9, and next a talk about the Egyptian data law is introduced in section 2.10. Finally, the chapter is concluded in section 2.11.

2.2 Medical & Health Records

Haux (2006) provided a definition of the medical record as a confidential repository maintained by healthcare professionals or organizations for each patient. This record encompasses the patient's personal details, such as name, address, and date of birth, along with a comprehensive overview of the individual's medical history. It also documents various events, including symptoms, diagnoses, treatments, and outcomes, incorporating relevant documents and correspondence. [2]

The utility of a medical record lies in its ability to empower health professionals to review past care events, make timely and informed clinical decisions, and formulate treatment plans geared toward minimizing risks and maximizing benefits for the patient. Originally, medical records existed in the form of paper documents, consolidating all patient information and being confined to specific hospitals or clinics. This iteration is referred to as Paper Medical Records (PMR), and patients faced challenges in transferring their profiles from one location to another. [3]

With the widespread adoption of computers, the concept of electronic medical records (EMR) emerged, retaining the essence of PMR but transitioning from paper to digital storage within healthcare facilities. As technology advanced and digitalization became more prevalent, the term Electronic Health Records (EHR) surfaced. EHR represents an evolved version of EMR, enabling users to access their profiles from various locations. Patients can conveniently view their records at any clinic or hospital. The following sections will delve into each approach, highlighting the respective advantages and disadvantages of paper medical records, electronic medical records, and electronic health records.

2.3 Paper Medical Records (PMR)

Paper medical records (PMR) refer to the traditional method of documenting and storing patient health information on physical paper. Pros of PMRs include simplicity and accessibility in low-tech environments, fostering a tactile connection for some healthcare providers. However, PMRs have notable cons, such as susceptibility to damage, loss, and inefficiency in data retrieval. They pose challenges for seamless information sharing, lack real-time updates, and can contribute to errors due to manual handling. Transitioning to electronic health records (EHR) addresses these drawbacks, offering improved accuracy, accessibility, and collaborative care, but may involve initial implementation costs and training challenges. [4]

2.4 Electronic Health Records (EHR)

Electronic Health Records (EHR) have emerged as a transformative force in healthcare documentation, representing a significant departure from traditional paper-based systems. The concept of EHR began taking shape in the 1960s with early experiments in computerized record-keeping. These nascent systems, however, were limited in scope and often confined to individual healthcare institutions. Over subsequent decades, advancements in technology and a growing awareness of the need for interoperability fueled the evolution of EHR into sophisticated, interconnected platforms capable of securely managing the entirety of a patient's medical information, including histories, diagnoses, medications, and treatment plans. The historical journey of the EHR mirrors the broader trajectory of technological innovation in healthcare. Early systems were rudimentary and often confined to individual institutions, limiting their potential for widespread impact. However, as technological capabilities advanced and the imperative for interoperability gained prominence, EHR systems evolved into more comprehensive solutions, fostering seamless communication and data sharing among diverse healthcare providers. In the contemporary healthcare landscape, the significance of EHR is multifaceted. At its core, EHR enhances patient care coordination by providing healthcare professionals with a unified and up-to-date view of a patient's medical history across various settings. This not only reduces the likelihood of medical errors but also facilitates more informed and personalized treatment decisions. Moreover, the EHR serves as a catalyst for improved communication and collaboration among healthcare providers, fostering a holistic approach to patient care. Beyond its immediate clinical implications, EHR plays a pivotal role in data-driven decision-making and quality improvement initiatives. The wealth of information housed within EHR systems enables healthcare organizations to analyze trends, identify areas for improvement, and implement evidence-based practices to enhance overall care quality. Additionally, the EHR facilitates the seamless integration of telehealth services, patient portals, and other digital health solutions, contributing to the ongoing evolution of modern health-

care delivery models. Crucially, EHR has become an essential tool in promoting patient engagement. Patients can actively participate in their healthcare journey by accessing their records, understanding treatment plans, and communicating with their healthcare providers through secure digital channels. This empowerment not only fosters a sense of ownership over one's health but also contributes to improved adherence to treatment regimens and better health outcomes. [5]

2.5 Blockchain and EHR

Blockchain technology has shown promise in the context of electronic health record (EHR) systems, particularly with Health Information Exchanges (HIE). The use of blockchain in healthcare systems offers compelling features such as accuracy, accountability, security, privacy, accessibility, and interoperability. However, there are challenges related to scalability, speed, file size limitations, regulatory data security concerns, and stability. Additionally, security and standardization are crucial aspects to consider for successful implementation. Blockchain can improve data sharing, patient-driven interoperability, and the overall efficiency and safety of patient care. However, challenges such as data throughput speed, file type and size restrictions, and data security need to be addressed. Furthermore, standardization efforts are essential for enabling more effective data exchange and addressing interoperability limitations with legacy systems. [6]

2.6 Blockchain

A blockchain can be referred to as a collection of records or open records that gets shared amongst participating parties. Every transaction that gets incorporated is first verified by all the participants in that transaction. Once the data is recorded by the blockchain, it can never be rewritten or changed. Thus, the blockchain can be termed a record book of all the transactions held. Cryptocurrencies, such as decentralized bitcoin or Ethereum, which can be termed peer-to-peer computerized cash, also use blockchain technology. [7]

Due to the continuous development of cryptocurrencies, the potential of the blockchain has gradually been discovered and has gained considerable attention in recent years. Blockchain technology, also known as distributed secure ledger technology, is a time-series data block that is interconnected to form a chain structure embedded with cryptography and distributed ledgers. Broadly speaking, blockchain technology uses blockchain data structures to validate and store data, distributed consistent algorithms to generate and update data, encryption to ensure data transfer and access security, and automated scripting code to form a new distributed infrastructure and computing paradigm associated with smart contracts. [7]

2.6.1 Blockchain Structure

At the core of the blockchain are units referred to as blocks. Blocks serve as the foundational units within a blockchain, comprising two main sections: the block header and the block body. The block body encapsulates a collection of transactions that are assembled to form a block. These transactions are organized in a Merkle tree structure within the block body. [8]

2.6.1.1 Block Header

The block header contains essential metadata crucial for the integrity and validation of the block. It typically includes:[8]
1) A reference to the previous block's hash, forming the chain of blocks.
2) A timestamp indicating the time of block creation.
3) A nonce (a random number) is used in the mining process for certain consensus algorithms like Proof of Work.
4) Other relevant information depends on the blockchain protocol.

2.6.1.2 Block Body and Transactions

The block body constitutes the core part of a block and primarily comprises numerous individual transactions. These transactions are bundled together in a Merkle tree format, ensuring efficient and secure verification of the block's contents. [8]

2.6.1.3 Merkle Tree Structure

The Merkle tree, also known as a hash tree, organizes transactions in a hierarchical structure of cryptographic hashes. This structure enables efficient verification and confirmation of transactions within a block. Each leaf node of the Merkle tree represents an individual transaction, while intermediate nodes are the hash values of their child nodes until reaching the root, which is a single hash value representing the entire set of transactions within the block. [8]

2.6.2 Decentralization

Blockchain technology does not rely on involvement by third parties or hardware, nor does it have any central control. All regular blockchain users can partake in the authentication of their data. As discussed previously, blockchain technology forms a network through a P2P protocol. Unlike the centralized network, nodes in a P2P network have the same network power, and there is no centralized server. [8]

Within a blockchain network, all participants, referred to as nodes, play an active role in the authentication and validation of data. Each node possesses equal network power, eliminating the hierarchical control or privileged authority that a centralized server might wield. This equality among nodes fosters a distributed

network where consensus mechanisms enable collective decision-making and agreement on the state of the ledger. In contrast to centralized networks, where a single point of control oversees data integrity and transaction validation, the decentralized nature of blockchain ensures that no single entity holds authoritative control. Instead, consensus algorithms facilitate agreement among nodes regarding the validity and order of transactions, enhancing security, transparency, and resilience within the network. This peer-to-peer structure not only mitigates the risks associated with single points of failure but also establishes a trustless environment where interactions and transactions are validated by the collective consensus of participants. Ultimately, decentralization in blockchain technology redefines the conventional approach to data management and validation, empowering users to actively engage in the verification and authentication of their data without relying on centralized authorities or hardware. [8]

2.6.3 Consensus Mechanism

Consensus mechanisms are vital for reaching agreement among distributed systems in blockchain, ensuring data accuracy across nodes. Decentralization enhances system stability but may affect efficiency, while centralized systems offer easier consensus but may compromise satisfaction. The choice of consensus (e.g., PoW, PoS, DPoS, PBFT) depends on business needs, serving as the backbone of cryptocurrency mining and ensuring valid transactions. Consensus mechanisms aim to prevent double-spending and resolve challenges in reaching an agreement. While no perfect mechanism exists, specific solutions cater to different scenarios, with Bitcoin's PoW paving the way for subsequent consensus methods. [8]

2.6.3.1 Proof of Work (PoW)

Satoshi Nakamoto, Bitcoin's creator, was able to bypass the problem by inventing the proof-of-work protocol. The protocol requires all nodes on the network to solve cryptographic puzzles by brute force. The miners solve cryptographic puzzles to mine a block in order to add it to the blockchain. This process requires an immense amount of energy and computational usage. The puzzles have been designed in a way that makes them hard and taxing on the system. When a miner solves the puzzle, they present their block to the network for verification. Verifying whether the block belongs to the chain or not is an extremely simple process. [8]

2.6.3.2 Proof of Stake(PoS)

Proof of stake protocol for block verification does not rely on excessive computations. It has been implemented for Ethereum and certain altcoins. Instead of splitting blocks proportionally to the relative hash rates of miners (i.e., their mining power), proof-of-stake protocols split stake blocks proportionally to the current wealth of

miners. The idea behind Proof of Stake is that it may be more difficult for miners to acquire sufficiently large amounts of digital currency than to acquire sufficiently powerful computing equipment. It is also an energy-saving alternative. [8]

2.6.4 Tokenization in Blockchain

Tokenization is the process of transforming the ownership and rights of particular assets into a digital form. Through tokenization, you can transform indivisible assets into token forms. [9]

2.6.4.1 Fungible Tokens

Fungible tokens are a type of cryptographic token that are identical and similar in nature and functionality. Two different fungible tokens serve the same purpose even when they are divided or exchanged with other fungible tokens of the same type. For instance, Bitcoin, the most popular cryptocurrency, is fungible. [9]

2.6.4.2 Non-Fungible Tokens (NFTs)

Non-fungible tokens (NFTs) are unique cryptographic tokens that exist on a blockchain and cannot be replicated. They can represent digital or real-world items like artwork and real estate. NFTs can represent individuals' identities, property rights, and more. Every NFT exhibits a different kind of functionality or aspect and is not comparable to other NFTs. [9]

2.7 Smart Contract

A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize both malicious and accidental exceptions, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud losses, arbitration and enforcement costs, and other transaction costs. [10]
It's simply a program stored on a blockchain that runs when predetermined conditions are met. [11]

2.7.1 How Smart Contracts Work

A smart contract—like any contract—is an agreement between two parties. Smart contracts use code to leverage the benefits of blockchain technology. The digital nature of smart contracts means they can be programmed to execute automatically in a six-step process. [12]

1. Parties agree to terms and conditions.

The creation of a smart contract starts with an agreement. The parties wishing to transact or exchange goods or services must agree on the terms and conditions of the arrangement. The parties involved must also decide how the smart contract will work, including what conditions must be met for the contract to execute and whether it will execute automatically.

2. The smart contract is created.

   The transacting parties have multiple options to create a smart contract, ranging from coding it themselves to working with a smart contract developer. The terms of the agreement are translated into a programming language to create the smart contract, which specifies rules and consequences just as a traditional legal contract would. Creating a smart contract can be simple, but it's important to note that a poorly designed smart contract is a major security risk. It's critical to fully verify the smart contract's security during this step.

3. The smart contract is deployed.

   Once the securely designed smart contract is ready, the next step is to deploy it to a blockchain. The smart contract is broadcast to the blockchain just like any other crypto transaction, with the code of the smart contract included in the transaction's data field. The smart contract is live on the blockchain once the transaction is confirmed, and it cannot be revoked or changed. That last part is important. Deploying a smart contract on a blockchain is like buying an item and intentionally throwing away the receipt. There are no returns, no refunds, and no exchanges—no exceptions.

4. Triggering conditions are met.

   A smart contract works by monitoring the blockchain or other credible information sources for certain conditions or triggers. These triggers can include almost anything that can be verified digitally—a date reached, a payment completed, a monthly bill received, or any other verifiable event. Trigger conditions may also be met when one or more parties to the contract perform a specific action.

5. The smart contract is executed.

   When the trigger conditions are satisfied, the smart contract executes. A smart contract that executes automatically may perform one or several actions, such as transferring funds to a seller or registering a buyer's ownership of an asset.

6. The contract result is recorded on the blockchain.

   The smart contract's execution is immediately broadcast to the blockchain. The blockchain network verifies the actions performed by the smart contract, records its execution as a transaction, and stores the completed smart contract on the blockchain. The record of the smart contract is generally available for review by anyone at any time.

2.7.2 Benefits of Smart Contracts

The smart contract has many advantages:[11]

- Speed, efficiency, and accuracy

  Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there's no paperwork to process and no time spent reconciling errors that often result from manually filling in documents.

- Trust and transparency

  Because there's no third party involved and because encrypted records of transactions are shared across participants, there's no need to question whether information has been altered for personal benefit.

- Security

  Blockchain transaction records are encrypted, which makes them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.

- Savings

  Smart contracts remove the need for intermediaries to handle transactions and, by extension, their associated time delays and fees.

2.7.3 Drawbacks of Smart Contracts

Using smart contracts also comes with risks. [13]

- Permanent

  They cannot be changed if there are mistakes.

- Human factor

  They rely on the programmer to ensure the code addresses the terms of the contract.

- Loopholes

  There may be loopholes in the coding, allowing contracts to be executed in bad faith.

2.8 Ethereum

Ethereum is a network of computers all over the world that follow a set of rules called the Ethereum protocol. The Ethereum network acts as the foundation for communities, applications, organizations, and digital assets that anyone can build and use. [14]
It is the foundation for building apps and organizations in a decentralized, permissionless, and censorship-resistant way. [15]
In the Ethereum universe, there is a single, canonical computer (called the Ethereum Virtual Machine, or EVM) whose state everyone on the Ethereum network agrees on. Everyone who participates in the Ethereum network (every Ethereum node) keeps a copy of the state of this computer. Additionally, any participant can broadcast a request for this computer to perform an arbitrary computation. Whenever such a request is broadcast, other participants on the network verify, validate, and carry out ("execute") the computation. This execution causes a state change in the EVM, which is committed and propagated throughout the entire network. [15]
Requests for computation are called transaction requests; the record of all transactions and the EVM's present state gets stored on the blockchain, which in turn is stored and agreed upon by all nodes. [15]
Cryptographic mechanisms ensure that once transactions are verified as valid and added to the blockchain, they can't be tampered with later. The same mechanisms also ensure that all transactions are signed and executed with appropriate "permissions" (no one should be able to send digital assets from Alice's account except for Alice herself). [15]

2.8.1 Ethereum Accounts

Ethereum has two account types: [16]

- Externally-owned account (EOA): controlled by anyone with the private keys.
- Contract account: a smart contract deployed to the network, controlled by code.

Both account types have the ability to:

- Receive, hold, and send ETH and tokens.
- Interact with deployed smart contracts.

2.8.1.1 Key differences between types of ethereum accounts

There are some differences between types of Ethereum accounts: [16]
Externally-owned

- Creating an account costs nothing.

- Can initiate transactions
- Transactions between externally owned accounts can only be ETH/token transfers.
- It is made up of a cryptographic pair of keys: public and private keys that control account activities.

Contract

- Creating a contract has a cost because you're using network storage.
- Can only send transactions in response to receiving a transaction
- Transactions from an external account to a contract account can trigger code, which can execute many different actions, such as transferring tokens or even creating a new contract.
- Contract accounts don't have private keys. Instead, they are controlled by the logic of the smart contract code.

2.8.2 What is Gas?

Gas refers to the unit that measures the amount of computational effort required to execute specific operations on the Ethereum network. Since each Ethereum transaction requires computational resources to execute, those resources have to be paid for to ensure Ethereum is not vulnerable to spam and cannot get stuck in infinite computational loops. Payment for computation is made in the form of a gas fee. The gas fee is the amount of gas used to do some operation multiplied by the cost per unit of gas. The fee is paid regardless of whether a transaction succeeds or fails. [17]

2.8.3 Relation between Smart Contract and Ethereum

Smart contracts are a type of Ethereum account. This means they have a balance and can be the target of transactions. However, they're not controlled by a user; instead, they are deployed to the network and run as programmed. User accounts can then interact with a smart contract by submitting transactions that execute a function defined on the smart contract. Smart contracts can define rules, like a regular contract, and automatically enforce them via code. Smart contracts cannot be deleted by default, and interactions with them are irreversible. Each instruction in the code has a gas cost (depending on how complex the instruction is). A transaction specifies and pays for a gas limit. If the gas used for execution exceeds the gas limit before a transaction finishes execution, any changes made by the transaction are reverted. The transaction can still be included in a block, and its gas cost will be collected by the miner as a fee.[18]

2.9 Hyperledger Fabric

The Hyperledger Project, hosted by the Linux Foundation since early 2016, is a collective initiative aimed at developing an industrial-grade, open-source distributed ledger framework and code base. This platform has the potential to revolutionize global business transactions. [19]
One of the projects incubating under the Hyperledger Project is Hyperledger Fabric. This is a distributed ledger platform designed for executing smart contracts, built on familiar and tested technologies. Its modular architecture allows for the pluggable implementation of various functions, enhancing its adaptability and versatility [20].

2.9.1 Hyperledger Fabric Ecosystem

The Hyperledger Fabric Ecosystem leverages the use of simple nodes, Docker containers, and Kubernetes pods in the following ways [21] :

Simple Nodes in Hyperledger Fabric: Hyperledger Fabric is a permissioned blockchain implementation that uses simple nodes for various roles such as peers, orderers, and Certificate Authorities (CAs). Each organization can have multiple peers, and each peer can have its own CouchDB instance.
Docker Containers: Hyperledger Fabric components are packaged into Docker containers. This includes the chaincode (smart contracts), which creates a container dynamically. Docker provides an easy way to package and distribute applications, which is why it's used in Hyperledger Fabric.
Kubernetes Pods: Kubernetes is used to manage these Docker containers. It simplifies managing containers in a cluster and provides a high availability of crucial fabric components like ordering services and fabric peers. If one container goes down, Kubernetes automatically creates another. This results in zero downtime for fabric containers.

2.9.2 Hyperledger Fabric Components

Hyperledger Fabric is a modular and extensible open-source system for deploying and operating permissioned blockchains. It provides a unique approach to consensus that enables performance at scale while preserving privacy. Here are the key components of Hyperledger Fabric [20] [22]:

- **Peer Node:** Manages the ledger, executes smart contracts, and participates in the consensus process.
- **Ordering Service:** Batches transactions into blocks and sends them to the committing peers.

- **Fabric CA:** The Fabric Certificate Authority (CA) issues a root certificate to member organizations and an enrollment certificate to each authorized user.
- **Ledger:** A distributed database that records all of the transactions that occur on the network.
- **Chaincode:** Specifies the rules for updating the ledger and determines which transactions are valid.
- **Channel:** A subset of network participants creates a private communication channel, visible only to those invited to it.
- **Organization:** In a Fabric blockchain network, an organization delineates boundaries and defines a Membership Service Provider (MSP) for the identities of administrators, users, peers, and orderers.
- **Endorsement Policy:** This refers to the conditions required for a transaction to be endorsed. A transaction is valid only if it has been endorsed in accordance with its policy.
- **Membership Services:** handles all the identity-related functions in a Hyperledger Fabric network.

2.10 Egyptian Data Law

Egypt has enacted a new set of data protection regulations, which were introduced in October 2020. The Personal Data Protection Law was approved on July 13, 2020, and made public on July 15, 2020. It was implemented on October 14, 2020, with the Executive Regulations anticipated to be released by April 14, 2021 [23].
This law introduces a range of compliance obligations and imposes substantial criminal penalties for non-compliance.

2.10.1 Definitions

The law defines 'personal data' as any information related to an identifiable individual, either directly or indirectly, through reference to any other data. This includes identifiers such as name, voice, image, identification number, online identifier, or any data that reveals psychological, health, economic, cultural, or social identity.
'Sensitive Personal Data' is classified as personal data that reveals psychological, mental, physical, or genetic health, biometric data, financial data, religious beliefs, political views, or a security situation. Personal data concerning children is considered to be sensitive personal data.

2.10.2 Processing of Personal Data

The law prohibits the processing of personal data without the consent of the data subject unless otherwise permitted by law. This ensures the protection of personal data and upholds the privacy rights of individuals.

2.11 Conclusion

In this chapter, an introduction to health records was provided, an overview of blockchain concepts was provided, and essential topics were introduced.
In the next chapter, the related work and many related techniques and technologies will be introduced. Also, related applications to our project and the need to extend related work will be introduced.

Chapter Three

3 Related Work

3.1 Introduction

In chapter 2, a general background about EHR and blockchain concepts was introduced as to how using blockchain could help in providing a better EHR privacy experience.
In this chapter, the research papers related to our project will be discussed, and a comparison between them will be made in section 3.2. The related applications to our project will be discussed in sections 3.3 and 3.4, with a comparison presented between them. The last two sections 3.5 and 3.6 will cover all the work focused on by our project, detailing what will be implemented. Finally, the chapter is concluded in Section 5.5.

3.2 Comparison Between Related Research Papers

In this section, a comparison between related research papers will be carried out according to some features:

1. Publishing Year: The publishing year refers to the year in which a research paper is officially released and made available to the public.
2. Citations: Citations are references to the number of other works (such as articles, books, or studies) that provide a way for authors to acknowledge and give credit to the sources that influenced or supported their work.
3. Journal Rank: To get information about the reputation of the journal in which the paper was published.
4. Blockchain Platform: A blockchain platform is a decentralized, distributed ledger technology that was used to enable secure and transparent recording of transactions across a network.
5. Documents Storage: It's allowed to store different document types like PDFs, images, etc.
6. Privacy: Privacy refers to the right of individuals to control their personal information and the extent to which their data is protected from unauthorized access or use.
7. Scalability: Scalability is the capability of a system, platform, or technology to handle increased workloads, data, or users without a significant decrease in performance.

8. Throughput: Throughput is a measure of the rate at which a system can process or transmit data.

9. Data Modifier: Data Modifier is the term for someone who can modify or add data to the blockchain.

10. Consensus Algorithm: A consensus algorithm is a crucial component that ensures all participants in a decentralized network agree on the state of the blockchain.

11. Smart Contracts: Smart contracts are self-executing contracts with the terms of the agreement directly written into code. They run on blockchain platforms automatically.

Features		[24]	[25]	[26]	[27]	[28]	[9]
Publishing Year		2023	2022	2023	2022	2020	2023
Citations		3	20	7	10	3	4
Journal Rank		Q2	Q3	Q2	–	–	Q1
Blockchain platform		HF	Ethereum	Ethereum	Ethereum	HF	Quorum
Documents Storage		**X**	✓	✓	**X**	✓	✓
Privacy		✓	✓	✓	✓	✓	✓
Scalability		✓	✓	✓	✓	✓	✓
Throughput		✓	✓	✓	✓	✓	✓
Public		**X**	✓	✓	✓	**X**	**X**
Data Modifier	**Doctors**	✓	✓	✓	✓	✓	✓
	Pharmacists	✓	✓	**X**	**X**	✓	**X**
	Patients	✓	✓	✓	✓	✓	✓
Consensus algorithm		Raft	voting	Raft	voting	voting	Raft
Smart contracts		✓	✓	✓	✓	✓	✓
ML Prediction tool		**X**	**X**	**X**	**X**	✓	**X**

Table 1: Comparison Between Related Research Papers

3.3 Related Applications

3.3.1 BurstIQ Health

BurstIQ Health is a trailblazer in revolutionizing healthcare data management through blockchain. Their platform, which is compliant with HIPAA and GDPR, ensures the secure storage of immutable health profiles. Noteworthy for seamlessly connecting disparate data sets, BurstIQ aligns perfectly with our project's focus on securing and managing patients' data. The platform's achievements, such as strategic partnerships and UN Global Compact admission, highlight its commitment to transformative solutions. BurstIQ transcends mere technology, embodying blockchain's disruptive potential by creating interconnected networks that empower patients, foster transparency, and drive positive change in healthcare data management. In essence, BurstIQ Health complements our project's vision, standing as a beacon for innovation in healthcare data security and patient empowerment.

3.3.2 Medicalchain

Medicalchain is a decentralized platform that enables the secure, fast, and transparent exchange and usage of medical data. It is built using the Hyperledger Fabric blockchain.

3.3.3 Patientory

It's a closed-source mobile application that works as a digital health data wallet by empowering patients with control of their health data so they can earn personalized reward-based payments to maximize their health.

3.3.4 MediBloc

MediBloc is developing a blockchain-based health information platform that provides patient-centric health information, reliable health information, and personalized health information with the vision of showing 'an innovative paradigm through developing a patient-centric health information solution and building a world of healthy lives for everyone.

3.3.5 MedRec

It's a free mobile app to manage medication plans, log health data, store medical documents, track symptoms, share information with doctors for remote consultations, and receive health advice and news.

3.3.6 OmniPHR

It's a distributed model to integrate PHRs for patients and healthcare providers. The scientific contribution is to propose an architecture model to support a distributed PHR, where patients can maintain their health history from a unified viewpoint, from any device, anywhere.

3.3.7 Doctor-y

It's a free and closed-source system that aims to provide a solution that will help in the digitalization and automation of the diagnosis process, to save patients' and physicians' time and help them reach more comfortability, and solve their problems.

3.4 Comparison Between Related Applications

In this section, a comparison between the related applications will be carried out according to some features:

1. EHR System That Stores Patients' Data: This feature encompasses the core functionality of storing and managing electronic health records (EHR). The system efficiently organizes and securely stores comprehensive patient data, ensuring accessibility and accuracy for healthcare providers.

2. QA Regulations: This feature ensures compliance with Quality Assurance (QA) regulations. It signifies that the system adheres to established standards and guidelines, promoting the quality, accuracy, and reliability of healthcare data.

3. Cloud Hosted Data: The system hosts patient data on the cloud, providing a scalable and accessible storage solution. Cloud hosting facilitates seamless data management, enabling healthcare professionals to access information securely from various locations.

4. Open Source: An open-source architecture allows for transparency and collaboration in software development. This feature signifies that the system's source code is accessible to the public, fostering innovation and enabling community-driven improvements.

5. Type of Blockchain: Specifies the type of blockchain technology utilized. Different blockchain types (e.g., public, secret).

6. Simple User Interface: A user-friendly interface designed for simplicity and ease of use. This feature enhances the user experience by providing an intuitive platform for healthcare professionals and patients, ensuring efficient navigation and task execution.

7. Appointments Calendar: Integrates a calendar system to manage and schedule appointments. This feature streamlines the process of booking and organizing appointments, enhances overall care coordination, and improves the patient experience.

8. Messaging: It incorporates a secure messaging system within the platform. Healthcare professionals can communicate efficiently, facilitating quick exchange of information for collaborative decision-making and improved patient care.

9. Smart Contract: Automated, self-executing contracts with predefined rules written in code. Implementing automated processes in healthcare, such as managing patient consent or facilitating secure data sharing,.

10. Compliance: Adherence to legal and regulatory standards in the healthcare sector. Ensure that your blockchain solution complies with data protection laws and other healthcare regulations.

11. Data Portability: The ability to transfer and access personal health data easily. Enabling patients to have control over their health data and share it securely between healthcare providers.

12. Consensus: Agreement among network participants on the validity of transactions. Choosing an appropriate consensus mechanism to ensure security and transparency in your healthcare blockchain.

13. Research Publications: peer-reviewed articles and papers related to healthcare blockchain and electronic health records. Referencing and building upon existing research to support the theoretical framework and methodology of your project.

14. Apply Data Analytics: Analyzing large datasets to extract meaningful insights. Using data analytics to gain valuable information from healthcare data stored on the blockchain could potentially improve patient outcomes.

15. Machine Learning Support: Integration of machine learning algorithms within the blockchain ecosystem. Enhancing healthcare analytics and decision-making by leveraging machine learning models on blockchain-stored data.

16. Virtual Visits: Remote healthcare consultations through digital platforms. Integrating virtual visits into the healthcare blockchain for secure and efficient telemedicine services.

Features	[29]	[30]	[31]	[32]	[33]	[34]	[35]
EHR System That Stores Patient's Data	✓	✓	✓	✓	✓	✓	✓
QA Regulations	✓	✓	✓	✓	✓	X	X
Cloud Hosted Data	✓	✓	✓	✓	✓	X	X
Open Source	X	X	X	✓	X	X	X
Type of Blockchain	S	P	P	P	P	S	X
Simple User Interface	✓	✓	✓	✓	✓	✓	✓
Appointments Calendar	X	X	X	X	✓	X	X
Messaging	X	✓	X	X	✓	X	X
Smart Contract	✓	✓	✓	X	X	✓	X
Compliance	HIPAA	HIPAA / GDPR	HIPAA	GDPR	HIPAA	GDPR	HIPAA
Data Portability	✓	✓	✓	✓	✓	✓	✓
Consensus	POS	POA	POW	POW / POS	POW	POW	—
Research Publications	✓	✓	✓	X	✓	✓	X
Apply Data Analytics	X	X	X	X	X	X	X
Machine Learning Support	X	X	X	X	X	X	X
Virtual Visits	X	✓	X	X	✓	X	✓

Table 2: Comparison Between Related Applications

3.5 Need to Extend Related Work

After reading and investigating some of the recent research papers and applications on health care applications, we need to apply this in Egypt, and we may conclude that there is a need for the following features:

1. There is a need to provide portability access to personal documents all the time.
2. There is a need to securely read the data from the patient or the doctor, store the data in CouchDB, and retrieve the data in a visualization way to the user.
   (a) Read the data from the patient or the doctor.
   (b) Store the data in CouchDB and files in the IPFS.
   (c) Retrieve the data in a visual way for the user.
3. There is a need to support Arabic users.
4. There is a need to allow the system to integrate with multiple organizations.
5. There is a need to make the system open source to allow different future contributions.
6. There is a need to make family channels to share the data of the family over their channel to be available in case of emergencies.
7. Selective disclosure, Patients can decide what information is sharable. [9]
8. There is a need to provide online consultation and messaging systems for easy and fast communication between doctors and their patients.
9. There is a need to provide an appointment calendar for scheduling doctor appointments.
10. There is a need to apply analysis and machine learning to data and give summaries to doctors which help in future research works.
11. Provide a solution that will help in the digitalization and automation of the diagnosis process Like Doctor Y.

3.6 Scope of Work

- Points 1, 2, 3, 4, 5, 6, 7, and 8 from the need to extend related work:
  1. Open source.
  2. Integrable with different organizations.
  3. Store and retrieve data securely using blockchain.
     - Read the data from the patient or the doctor.
     - Store after tokenization by smart contract and files in the IPFS.
  4. Emergency.
  5. Sharing Data.
  6. Arabic support.
  7. Online consultation and Messaging system.
  8. Website and mobile application.
  9. Documentation by writing the report.

3.7 Conclusion

In this chapter, related work and related applications to the use of blockchain technology to save the EHR of patients were introduced, and at the end of this chapter, we showed what features our project is focusing on.
In the next chapter, we will talk about the requirements and the design of the project.

Chapter Four

4 Development process

4.1 Introduction

In chapter 3, a discussion about the related work and related applications of using blockchain to save the EHR of patients is introduced.
In this chapter, The development process of the project will be shown which is the Software Process Improvement (SPI) model. Finally, the chapter is concluded in Section 4.3

4.2 Software Process Improvement (SPI)

4.2.1 What is SPI?

The Software Process Improvement (SPI) model was developed by the Software Engineering Competence Center (SECC) to assist small and medium-sized enterprises in enhancing the quality of their products to meet international standards. This is achieved by adopting contemporary software development processes and practices in a cost-effective manner .
SPI encompasses five key processes: project management, product development, peer review, quality assurance, and configuration management. These processes are implemented across four phases of a project:

- **Initiation**: Focuses on defining the project scope, identifying stakeholders, and creating a preliminary project management plan.
- **Planning**: Involves developing a detailed project plan that includes a schedule, estimates of size, effort, and cost, as well as a risk management plan.
- **Execution, Monitoring, and Control**: Entails executing the project plan, managing resources, tracking progress, and making necessary adjustments.
- **Closing**: Involves finalizing the project and resolving any remaining issues.

Each SPI process involves specific tasks for each phase and generates certain work products (outputs). Since this project is academic rather than commercial, not all SPI processes were applied. We adapted the SPI model to suit the nature of the project, and this chapter provides a summary of the adapted processes we utilized. [36]

4.2.2 Project Management Process (PMP)

The project management process is a methodical approach to planning, organizing, and managing resources to achieve specific project objectives. This framework helps in defining project activities, monitoring progress, and implementing corrective actions when necessary. By adhering to a structured process, project managers can enhance the likelihood of successfully meeting the project's goals and objectives.

For our project, we created four key work products:

- **Minutes of Meetings (MoM)**: After each meeting, we prepared MoM documents that recorded the meeting's location and time, attendees, main discussion points, action items to be completed by the next meeting, and the agreed-upon location and time for the next meeting.
- **Process-Activity-Task Matrix (PATM)**: We developed a PATM that outlined the main processes involved in project development. Each process was broken down into smaller units called activities, which were further subdivided into specific tasks. (see Table 3)
- **Weekly Time Sheets**: This sheet detailed the tasks each team member worked on every week and the number of hours spent on each task. This approach facilitated tracking the collective contributions and managing the project's progress effectively.
- **Implementation Plan**: We prepared a comprehensive Implementation Plan that detailed each task's estimated start and end dates, assigned responsibilities, and completion status. This plan not only outlined the timeline for each task but also specified who was responsible for each task and included a progress percentage to track the completion of each task. This structured approach ensured clarity in task management and facilitated effective monitoring of the project's progress. [36]

4.2.3 Product Development Process (PDP)

The product development process encompasses all engineering activities that transform customer requirements into a final product through a series of steps. This process operates under the supervision of the project management process and is supported by peer review, quality assurance, and configuration management processes.

The product development process includes numerous procedures such as requirements planning, requirements elicitation, requirements analysis, requirements development, requirements validation, requirements acceptance, requirements management, development planning, architecture designing, detailed designing, implementation, component testing, integration testing, system testing, acceptance testing, and finally, product release.

Process	**Activity**	**Task**
Establishing Requirements	Patient experience	Make interactive questionnaires with patients Gather features from various other apps
	Medical provider experience	Making interviews for some doctors
	Non-functional requirements	Define security parameters Define our scalability limits and requirements
Blockchain and architecture	Network Setup and Configuration	Set up the Hyperledger Fabric network infrastructure Configure the network nodes Establish communication channels between nodes
	Chaincode Development and Deployment	Develop smart contracts (chaincode) based on defined business logic Package chaincode for deployment on Hyperledger Fabric
	Monitoring and Maintenance	Implement monitoring tools for tracking network performance Set up alerts for potential issues or security breaches
App Implementation	Planning and Scope Definition	Define project goals, objectives, and scope for both mobile and web platforms Identify key stakeholders and establish communication channels
	Technology Stack Selection	Evaluate and choose appropriate technologies for mobile and web development Consider factors like platform compatibility, user experience, and scalability
	User Interface (UI) and User Experience (UX) Design	Create wireframes and design mockups for both mobile and web interfaces Ensure consistent branding and a seamless user experience across platforms
	Back-End Development	Develop the back-end infrastructure to support both mobile and web applications
	Front-End Development	Build the user interfaces for mobile and web applications based on the design specifications Implement responsive design for optimal viewing on various devices
Publication	Open source	Publish public organization repos on GitHub with user-friendly usage guide
	Documentation	Well organized report with references for all resources used Declarative presentation

Table 3: Process-Activity-Task Matrix

In the development of this project, several of these procedures were implemented to ensure the high quality of the final product, resulting in the following outputs:

- **Software Requirements Specifications (SRS)**: This document outlines the functional and non-functional requirements of the project. It serves as a detailed guideline for the development team, ensuring that all customer needs and expectations are clearly defined and met. The SRS includes use cases, user stories, and specific requirements for performance, security, and usability.
- **Architecture and Detailed Design**: This output includes the architectural design of the system, detailing the overall structure and how the different components interact with each other. The detailed design further breaks down each component, providing specific information about the design patterns, data structures, and algorithms to be used. This document serves as a blueprint for the development team, guiding the implementation phase and ensuring consistency and coherence in the system's design.
- **Test Plan**: This plan outlines the testing strategy and procedures to ensure that the final product meets the specified requirements and is free of defects. It includes various types of testing, such as component testing, integration testing, system testing, and acceptance testing. The test plan specifies the testing environment, tools, test cases, and expected outcomes. It ensures that all aspects of the product are thoroughly tested and validated before release.

By meticulously following these procedures and producing these documents, we aimed to achieve a high-quality final product that meets all specified requirements and provides a reliable and effective solution for the users. [36]

4.2.4 Peer Review Process (PRP)

The peer review process aims to detect and remove defects from work products early in the development cycle through a systematic examination by the author's peers.

In our project, in addition to the timesheets detailing each team member's tasks as discussed in the project management process, we implemented peer review documents. These documents listed each task identified the task owner, specified the peer reviewer, and documented any problems detected by the peer reviewer.

This peer review process facilitated thorough scrutiny of our work, enabling us to promptly identify and address any issues. By leveraging everyone's knowledge, we enhanced the quality of our work and minimized the likelihood of encountering problems later on.

4.2.5 Configuration Management Process (CMP)

The configuration management process ensures a secure infrastructure for the entire project and the software development life cycle by storing all evolving work products

in a controlled environment.

In our project, two primary tools were utilized for configuration management:

- **GitHub**: This platform was employed for configuration management and version control of the project source code. It allowed us to track changes, collaborate on code development, and maintain a history of revisions.
- **Google Drive**: We used Google Drive to store all project-related documents, maintaining all versions of these documents. This facilitated easy access and sharing of project documentation among team members, ensuring everyone had access to the most up-to-date information.

4.3 Conclusion

In this chapter, The development process of the project will be shown which is the Software Process Improvement (SPI) model.
In the next chapter, we will talk about software requirements, system design, and the architecture of that project.

Chapter Five

5 Requirements and Design

5.1 Introduction

In chapter 4, a discussion about the development process has been followed is introduced.
In this chapter, The requirements and design of the project will be shown. Finally, the chapter is concluded in Section 5.5.

5.2 Software Requirements Specifications(SRS)

5.2.1 Scope of the Software

- Blockchain Integration: Implement blockchain technology to create a secure and decentralized system for storing and managing healthcare records.
- Security and Confidentiality: Prioritize the confidentiality and security of healthcare records by leveraging the cryptographic features and decentralized structure of blockchain to prevent unauthorized access, data breaches, and compromises in patient privacy.
- Immutability and Tamper-Proofing: Utilize blockchain's immutable nature to ensure that healthcare records are tamper-proof, maintaining the integrity of patient information.
- Transparent and Accountable: Introduce transparency and accountability into healthcare data management through the decentralized nature of blockchain, providing a clear audit trail of record access and modifications.
- Migration Analysis: Conduct an in-depth analysis of the benefits and challenges associated with migrating from traditional centralized healthcare databases to a distributed ledger-based framework.
- Viability and Feasibility Assessment: Evaluate the viability and feasibility of blockchain-based healthcare record systems, considering factors such as scalability, interoperability, and regulatory compliance.
- Transformational Potential: Explore the potential of blockchain technology to transform the healthcare landscape by fostering trust, enhancing security, and safeguarding patient confidentiality.

- Contributions to Discourse: Provide significant insights and contributions to the discourse on utilizing cutting-edge technology to fortify data security and privacy in healthcare, contributing to the advancement of the field.

5.2.2 System Specifications

5.2.2.1 User Requirements

- As a user, I want to easily create an account with just a few simple steps. I should feel welcomed and guided through the registration process, making it a seamless and user-friendly experience.
- As a user, I want to log in and see all the data I have entered and be able to edit it.
- As a user, I want the assurance that my health data is a private sanctuary. I should be the guardian of who accesses my information, ensuring that my personal health details remain confidential and secure.
- As a user, I want to dive into the story of my health. I should be able to explore and see all my medical history including the medical tests, x-rays, and chronic diseases.
- As a user, I appreciate a platform that respects my language and cultural background. I should be able to navigate and understand the system in my preferred language, fostering a sense of inclusivity and comfort.
- As a user, I appreciate having a direct line to my healthcare provider. I want the ability to seamlessly communicate with my doctor through an integrated messaging system within the application.
- As a user, I want to be able to search for doctors or laboratories in the system to ease contact with them.
- As a doctor in the system, I want to be able to see all the medical history of the patients to make a good examination of them and be able to write the best cure for them.

5.2.2.2 Functional Requirement

1. User Registration and Authentication
    - Users should be able to register securely.
    - The system must authenticate users before providing access to their health data.
2. Data Entry and Update

- Doctors and Laboratories can input new health data about the patients.
- Ensure the system supports various data types (medical records, test results, prescriptions, etc.).

3. Selective disclosure
   - The patient should be able to decide what information to share.
4. Blockchain Integration
   - Utilize blockchain technology for storing and securing health data.
   - Implement smart contracts to enforce data access rules.
5. Data Access and Control
   - Patients should have full control over who can access their health data.
6. Data Encryption
   - Ensure end-to-end encryption for all data transmissions.
   - Encrypt sensitive health information stored in the blockchain.
7. Messaging System
   - To make it easy for the doctor and the patient to communicate.

5.2.2.3 Non-Functional Requirement

1. Security
   - The system must comply with industry-standard security protocols.
   - Regular security audits and updates should be conducted.
2. Performance
   - The system should provide low-latency access to health data.
   - Handle a large number of simultaneous users.
3. Scalability
   - Design the system to accommodate an increasing number of users and data volume.
4. Usability
   - Ensure a user-friendly interface for both technical and non-technical users.
   - Provide clear instructions for data management.
5. Reliability

- The system must be available and reliable 24/7.
- Implement backup and recovery procedures.

6. Compliance
    - Ensure compliance with healthcare data protection regulations (HIPAA, GDPR, etc.).
    - Regularly update the system to comply with evolving regulations.
7. Interoperability
    - The system should integrate seamlessly with existing healthcare information systems.
8. Documentation
    - Maintain comprehensive documentation for system configuration, APIs, and data structures.

5.3 Software Design and Architecture

5.3.1 Work overflow

The workflow diagram illustrates the sequence of activities for different user roles within the system, including patients, doctors, lab technicians, and emergency personnel. Each role has a distinct set of actions they can perform, ensuring a streamlined and organized process for accessing and managing healthcare data.

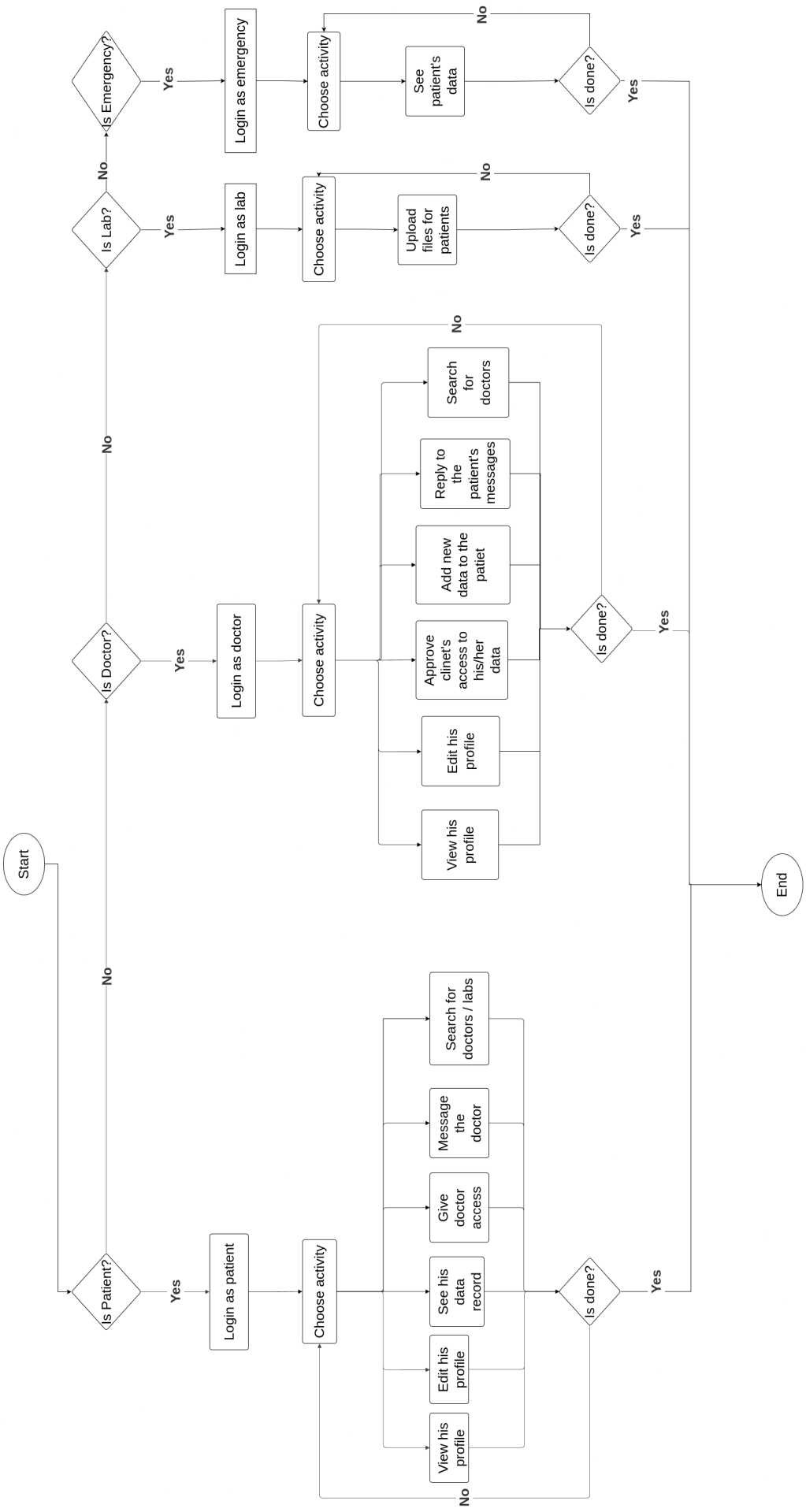

Figure 1: Work overflow

5.3.2 Hyperledger network

The implementation of our system utilizes a Hyperledger Fabric network, designed to facilitate secure and efficient data management across various healthcare organizations. The network is structured into multiple organizations, each representing a distinct participant in the healthcare ecosystem, including patients, laboratories, doctors, hospitals, and an ordering service.

5.3.2.1 Key Components

- **Organizations**
  - **Patient Org:** Manages patient data with peers responsible for maintaining the ledger.
  - **Laboratory Org:** Handles laboratory data and interacts with its own peers.
  - **Doctor Org:** Focuses on doctors' interactions and data management with dedicated peers.
  - **Hospital Org:** Manages hospital-related data and operations.
  - **Orderer Org:** Facilitates the ordering service, ensuring the consensus and order of transactions across the network.
- **Channels**
  - **Channel 1:** The primary channel for general communication among all organizations.
  - **Other channels** Specific channels for targeted interactions and data exchange between selected organizations.
- **Data Storage**
  - **CouchDB:** Utilized for the storage of ledger data in a structured manner.
  - **IPFS:** Employed for decentralized file storage, enhancing data accessibility and security.
- **Supporting Components**
  - **APIs and API Gateway:** Facilitate secure communication between the compute server and the Hyperledger Fabric network.
  - **HLF Operator Server:** Manages the operations and interactions within the network, ensuring smooth execution of contracts and transactions.

This robust network design ensures that data integrity, security, and privacy are maintained while allowing efficient interaction among various entities within the healthcare system.

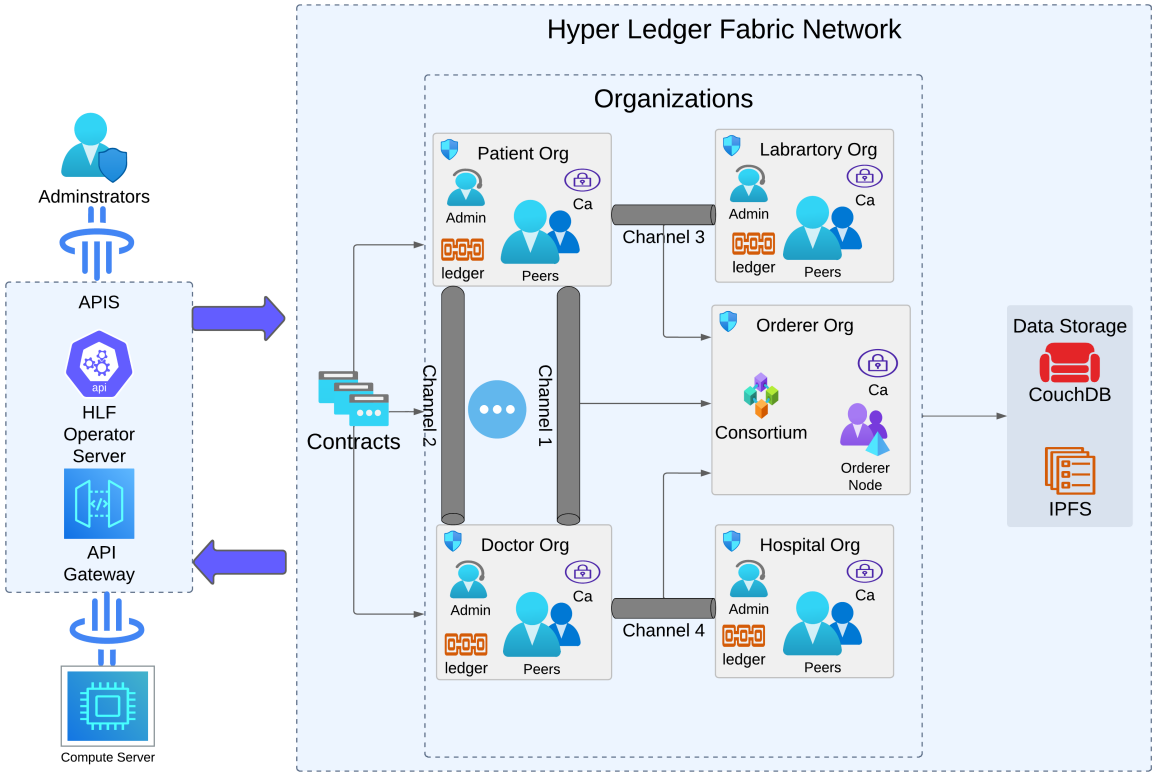

Figure 2: Hyperledger network

5.3.3 Database Design

Our database is structured using MongoDB, reflecting a document-oriented design rather than a traditional ER (Entity-Relationship) model. The diagram illustrates the relationships and data fields for various entities, such as patients, doctors, visits, and other key components within the healthcare system.

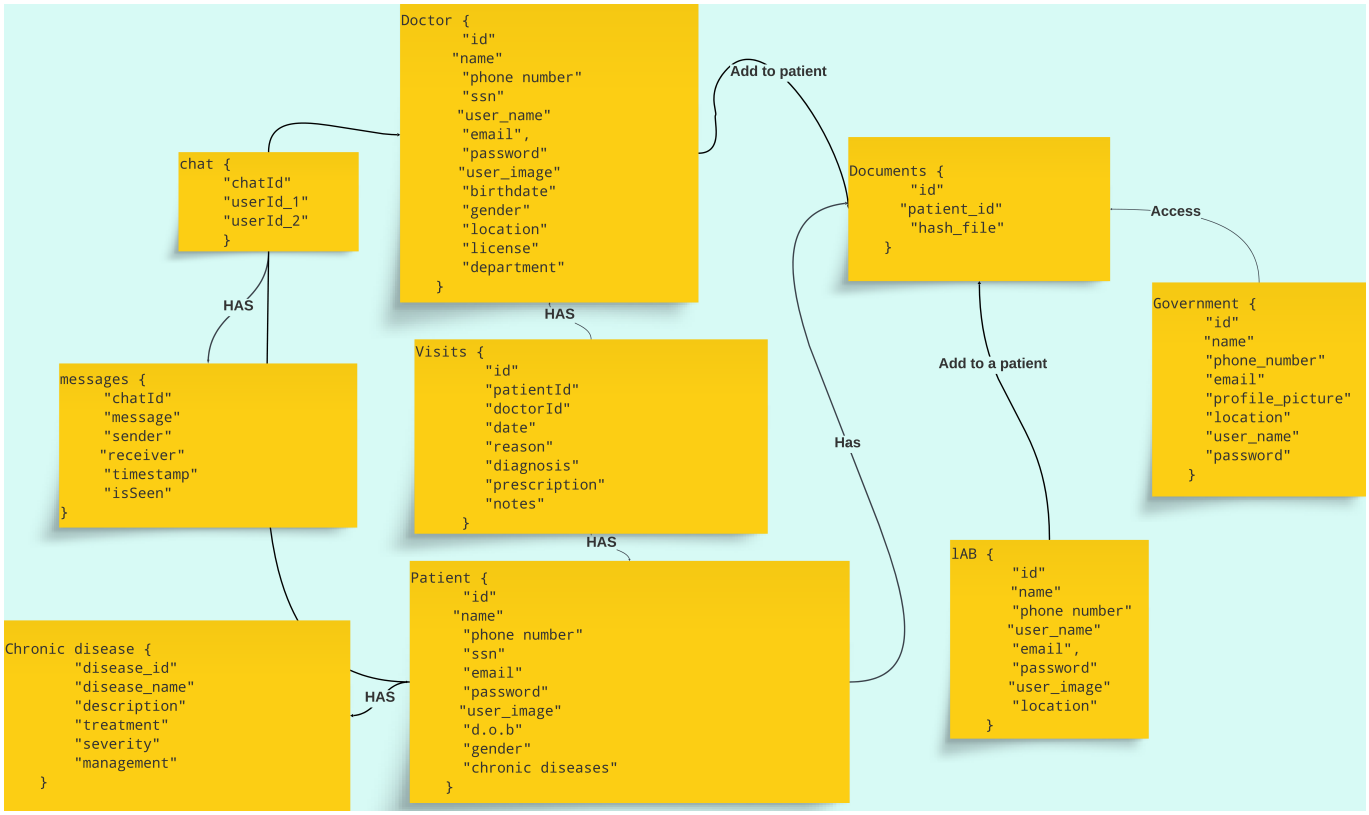

Figure 3: Database Design

5.3.4 Sequence Diagrams

Sequence diagrams are a type of UML diagram used to illustrate how objects interact in a particular sequence over time. They provide a visual representation of the flow of messages between various components within a system, highlighting the order in which these interactions occur. All of the prepared sequence diagrams can be found in Appendix B. A sample of the sequence diagrams is shown here. It's for showing how the patient can give access to the doctor to see his/her data.

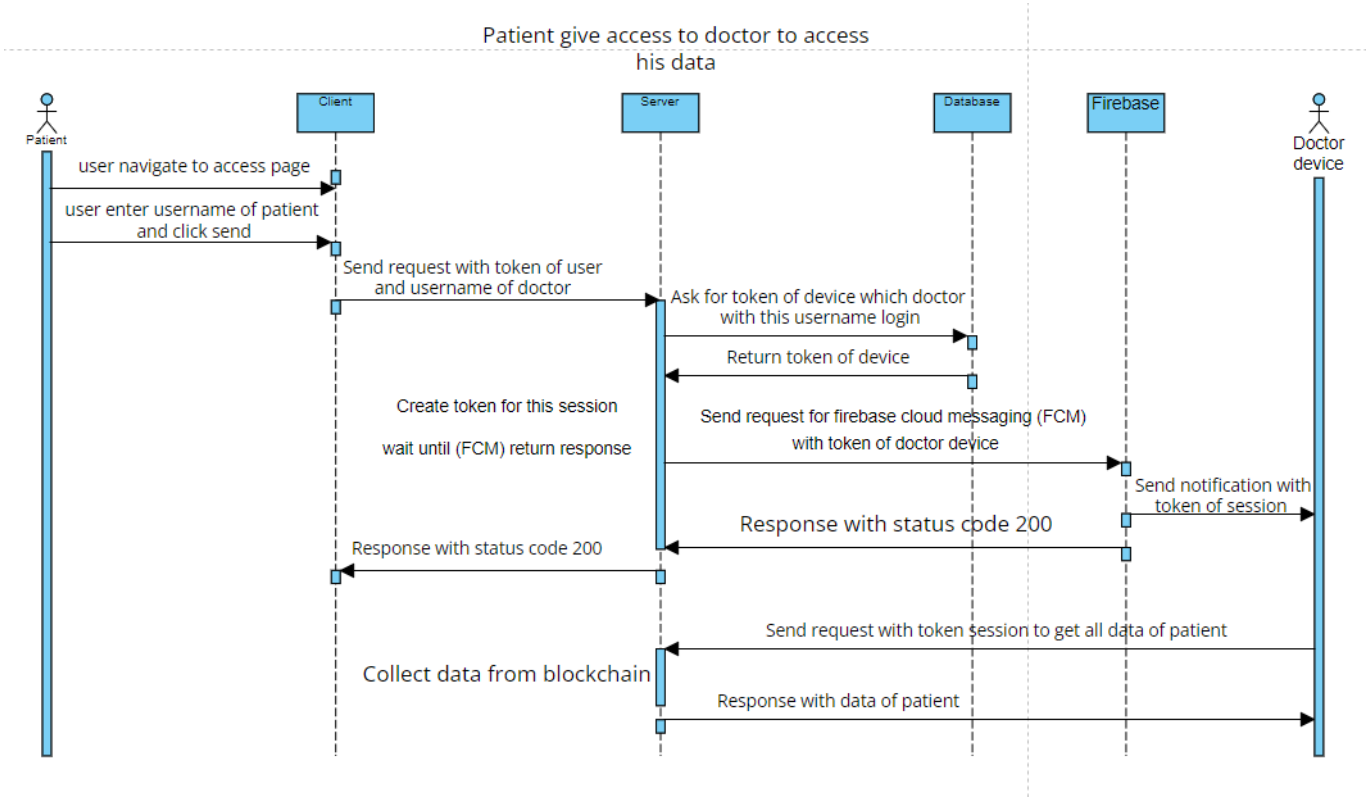

Figure 4: A sample sequence diagram showing how to give access to the doctor on the patient's data

5.4 Platforms and Tools

5.4.1 Front-end Tools

5.4.1.1 Flutter[37]

Flutter is an open-source UI software development kit created by Google. It is used to develop cross-platform applications from a single codebase for any web browser, including Fuchsia, Android, iOS, Linux, macOS, and Windows. First described in 2015, Flutter was released in May 2017. [38]

5.4.2 Back-end Tools

5.4.2.1 Node.js[39]

Node.js is a cross-platform, open-source JavaScript runtime environment that can run on Windows, Linux, Unix, macOS, and more. Node.js runs on the V8 JavaScript engine and executes JavaScript code outside a web browser. [40]
It has many frameworks that can be used to make good backend web applications, like Express.js. Express.js, or simply Express, is a back-end web application framework for building RESTful APIs with Node.js, released as free and open-source software under the MIT License. It is designed for building web applications and APIs. It has been called the de facto standard server framework for Node.js. [41]

5.4.2.2 MongoDB[42]

MongoDB is a source-available, cross-platform, document-oriented database program. Classified as a NoSQL database product, MongoDB utilizes JSON-like documents with optional schemas. MongoDB is developed by MongoDB Inc. and current versions are licensed under the Server Side Public License (SSPL). MongoDB is a member of the MACH Alliance. [43]

5.4.3 Blockchain tools and platforms

5.4.3.1 Hyperledger Fabric[44]

Hyperledger Fabric is an open-source, permissioned blockchain framework, started in 2015 by the Linux Foundation. It is a modular, general-purpose framework that offers unique identity management and access control features, which make it suitable for a variety of industry applications such as track-and-trace of supply chains, trade finance, loyalty, and rewards, as well as clearing and settlement of financial assets. [45]
There are many platforms that can be used to write code on it, like Node.js

5.4.3.2 Kaleido Platform

Kaleido provided us with a user-friendly interface and robust infrastructure, streamlining the deployment process. Additionally, Kaleido offers APIs that allow us to easily interact with the deployed contract, facilitating seamless integration and interaction with our blockchain application.

5.4.4 Version Control

5.4.4.1 Git[46]

Git is a distributed version control system that tracks changes in any set of computer files, usually used for coordinating work among programmers who are collaboratively developing source code during software development. Its goals include speed, data integrity, and support for distributed, non-linear workflows (thousands of parallel branches running on different computers). [47]

5.5 Conclusion

In this chapter, the software requirements, system design, and architecture were introduced, and at the end of this chapter, we showed what platforms and tools will be used to implement the project.
In the next chapter, we will talk about the Implementation, results, and conclusion of our project.

Chapter Six

6 Implementation and Results

6.1 Introduction

In chapter 5, a discussion about the requirements and design considerations for our project is introduced.
In this chapter, Implementation details and results will be shown. Finally, the chapter is concluded in Section 6.4.

6.2 Implementation

6.2.1 Chaincode

The process as shown in Figure 5 starts with implementing the chaincode, followed by packaging it into a format suitable for deployment. The packaged chaincode is then uploaded over the network. Once uploaded, it is deployed to a specific channel within the blockchain network. After deployment, a URL for the chaincode is generated. This URL is used to integrate the chaincode with backend services, enabling interaction with the deployed smart contract through provided APIs.

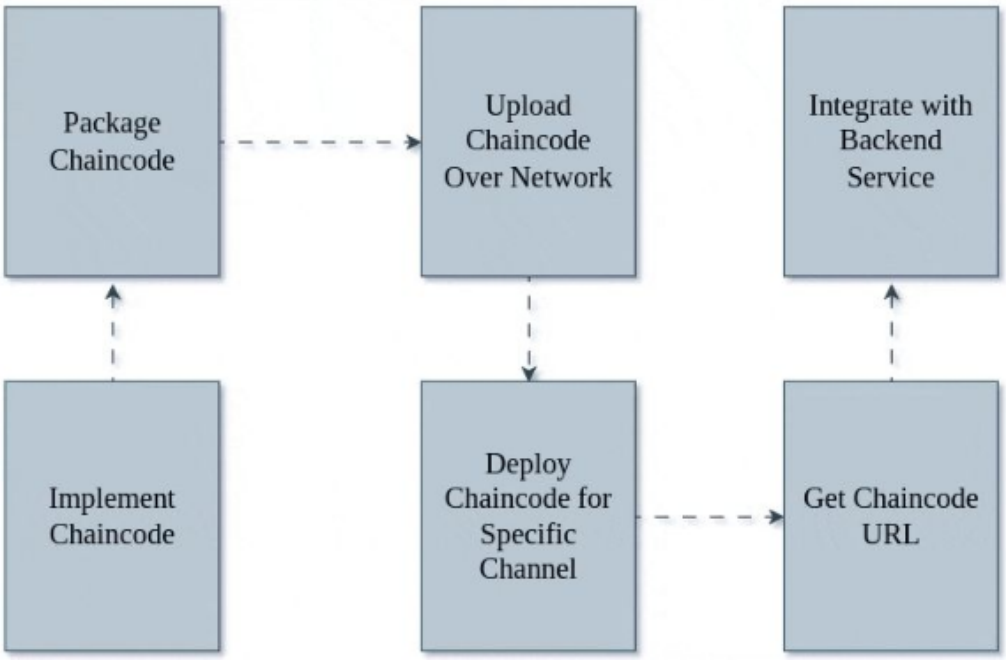

Figure 5: Contract Flow

6.2.2 Features

1. Registration system

Description: The registration system in our Rosheta app caters to four main types of users: patients, doctors, labs, and emergency responders. Each user type has a distinct registration flow to ensure the collection of relevant information and to provide access to the appropriate features within the app.

Patients: Patients can sign up using their personal information, medical history, and contact details. They gain access to features like booking appointments, viewing prescriptions, and interacting with healthcare providers.

Doctors: Doctors register by providing their medical credentials, practice information, and specializations. This ensures that only verified medical professionals can offer consultations and manage patient care within the app.

Labs: Laboratories register by submitting their accreditation details and services offered. This allows them to receive test requests from doctors and patients and provide results directly through the app.

Emergency Responders: Emergency responders register with their credentials and service areas, enabling them to respond to urgent medical situations reported through the app.

Session Management: To ensure secure and efficient session management, we utilize JWT (JSON Web Tokens). JWT tokens are issued upon successful authentication and are used to handle user sessions, maintaining security and scalability.

Comparison with Other Apps: Unlike other related apps, our Rosheta app offers a comprehensive and unified registration system for multiple user types, ensuring seamless interaction between patients, doctors, labs, and emergency responders. Additionally, the use of JWT tokens for session management provides a higher level of security and performance compared to traditional session handling methods. Many other apps might limit their focus to a single user type or lack the integrated session management capabilities we offer.

UI Samples: For a visual representation of the registration process, please refer to the UI sample screenshots in the Appendix C: Registration System.

2. Profile

Description: Each user in the Rosheta app has a profile page where they can manage their personal information. Users can modify their data as needed and have the option to control the visibility of their critical data.

Patient Profile: Patients can update their personal details, medical history, and contact information. They have the option to show or hide critical data based on their preferences.

Doctor Profile: Doctors can manage their professional information, including their credentials, practice details, and specializations. Patients searching for doctors can view doctor profiles to find the best match for their needs.

Lab Profile: Labs can update their accreditation information, services offered, and contact details. This ensures that both patients and doctors have access to accurate and up-to-date lab information.

Emergency Responder Profile: Emergency responders can manage their credentials and service areas, ensuring that their profiles provide accurate information for those in need of urgent assistance.

Privacy Controls: Users have control over their profile data, allowing them to choose which information to display publicly and which to keep private. This ensures user privacy and data security while maintaining the functionality of the app.

Comparison with Other Apps: We have added privacy controls to enhance the user experience.

UI Samples: For a visual representation of the profile management interface, please refer to the UI sample screenshots in the Appendix C: Profile screens.

3. Chat

Description: The chat feature in the Rosheta app facilitates direct communication between different types of users, enhancing collaboration and support within the healthcare ecosystem.

Patient Chat: Patients can initiate chats with doctors, labs, or emergency responders. This allows patients to seek medical advice, inquire about test results, or request urgent assistance.

Doctor Chat: Doctors can start chats with patients, other doctors, labs, and emergency responders. This enables doctors to coordinate care, consult with colleagues, discuss lab results, and manage emergency situations.

Lab Chat: Labs have the ability to initiate chats with patients, doctors, other labs, and emergency responders. This helps labs to provide test results, seek clarifications on test requests, and ensure timely communication in emergency cases.

Emergency Chat: Emergency responders can initiate chats with patients, doctors, labs, and other emergency responders. This facilitates rapid communication during medical emergencies and ensures a coordinated response.

Communication Channels: The chat system supports text messaging, file sharing, and real-time notifications, making it a versatile tool for effective communication within the app.

Comparison with Other Apps: Not all the related apps have chat in their implementations, so we added this feature to facilitate communication between the users in one app.

UI Samples: For a visual representation of the chat interface, please refer to the UI sample screenshots in the Appendix C: Chats screens.

4. Search

Description: The search feature in the Rosheta app allows users to quickly and efficiently find relevant information and services. Users can search for doctors, labs, emergency responders, and other patients. Advanced search filters enable users to refine their searches based on criteria such as location, specialization, availability, and user ratings.

Comparison with Other Apps: We have added many filters to enhance the search results and experience.

UI Samples: For a visual representation of the search interface, please refer to the UI sample screenshots in the Appendix C: Search screens.

5. Sharing Data

Description: The data sharing feature in the Rosheta app enables patients to share their medical data with doctors and labs securely and efficiently. The patient maintains full control over their data.

Process: (a) A doctor sends a data-sharing request to the patient. This request includes a one-time password (OTP) to ensure security.

(b) The patient receives a notification about the request. They can then choose to accept or deny the data-sharing request.

(c) If the patient accepts, the doctor gains access to the patient's medical data.

(d) The doctor can now add records to the patient's profile or view the patient's complete medical history, facilitating better-informed medical decisions and ongoing care.

Patient Control: The patient is the sole controller of their data, ensuring privacy and security. No data is shared without the patient's explicit consent.

Comparison with Other Apps: We used the OTP idea inspired by the bank transactions to make it easy and seamless for the patient to share their data, in related apps they used other ideas like QR or NFC bands which are feasible and give good user experience too but we decided to go with the OTP idea as it doesn't need any hardware or additional s.w.

UI Samples: For a visual representation of the data sharing interface, please refer to the UI sample screenshots in the Appendix C: Sharing data.

6. Document Handling

Description: The document handling feature in our Rosheta app leverages IPFS (InterPlanetary File System) for storing and retrieving various types of documents, including PDFs, images, and other file formats. IPFS is a decentralized protocol that provides a resilient and efficient way to manage and share content across the internet.

IPFS Integration: We utilize IPFS to ensure that documents uploaded by users, such as medical reports, diagnostic images, and treatment plans, are securely stored and accessible. IPFS hashes are used to uniquely identify each document, making it easy to retrieve and verify the integrity of the content.

User Accessibility: Patients, doctors, labs, and emergency responders can upload and access documents directly through the Rosheta app. This seamless integration ensures that relevant medical information is readily available when needed for consultations, diagnostics, or emergency situations.

Advantages of IPFS: By utilizing IPFS, we enhance data security and availability. Documents are distributed across a network of nodes, reducing the risk of data loss or unauthorized access. Additionally, IPFS supports efficient content delivery through its decentralized architecture, improving performance compared to traditional centralized storage solutions.

Comparison with Other Apps: Utilizing the IPFS for storing the documents was a unique idea in such applications, others use cloud storage or their servers for that purpose.

UI Samples: For a visual representation of the document handling interface, including uploading and accessing documents via IPFS, please refer to the UI sample screenshots in the Appendix C: Documents.

7. Emergency Cases

Description: In emergency situations, the app provides emergency responders with immediate access to patient data without the need for a permission token. This ensures that critical information is available when it is needed the most.

Process: (a) Emergency responders access the patient's data directly through the app in urgent situations.

(b) A notification is sent to the patient informing them that their data has been accessed by an emergency responder. This keeps the patient informed and ensures transparency.

Comparison with Other Apps: Other apps don't provide this emergency access but we thought that being totally private is worthless in emergency cases.

UI Samples: For a visual representation of the emergency access interface, please refer to the UI sample screenshots in the Appendix C: Emergency.

6.3 Results

in the Table below we show a stress test on the network, and from the results, we conclude that the implementation with the blockchain is feasible.

Samples	Avg Latency (ms)	Throughput (Trs/sec)
1	431	2.3000
10	243	5.4555
100	1051	41.4250
1000	13606	32.3394

Table 4: Latency and Throughput for Endorsing a Contract Transaction

6.4 Conclusion

In this chapter, the software requirements, system design, and architecture were introduced, and at the end of this chapter, we showed what platforms and tools will be used to implement the project.
In the next chapter, we will talk about the Implementation, results, and conclusion of our project.

Chapter Seven

7 Conclusion and future work

7.1 Introduction

In the previous chapters, the project details were discussed thoroughly. The motivation for the project, the scientific background needed, the literature review, the need to extend the related work, the scope of work, the requirements and design, the followed development process, the implementation details and results all are discussed. In this chapter, the Conclusion, contribution of the project, and the proposed future work will be discussed.

7.2 Project Conclusion

In this project, we developed "Rosheta," a comprehensive platform designed to revolutionize medication management and healthcare accessibility. Throughout the project phases, from inception to implementation, we addressed critical aspects to enhance medication adherence and streamline healthcare delivery.

In conclusion, "Rosheta" represents a significant advancement in the field of digital healthcare solutions, offering a scalable platform to enhance medication adherence and patient care management. By leveraging cutting-edge technologies and user-centric design principles, we aim to empower individuals and healthcare providers alike in managing health outcomes effectively.

7.3 Contribution Summary

The contribution of our work is fourfold:

7.3.1 Ensuring Security and Privacy Compliance

- Utilize Hyperledger Fabric and tokenization in chain code development to comply with Egyptian data laws.
- Establish the network using Spydra for robust security.
- Deploy the chaincode over the Spydra network to ensure comprehensive security and privacy.

7.3.2 Tailored Application Development for Egyptian Users

- Develop an application customized for Egyptian users.
- Provide Arabic language support within the application interface.

- Incorporate secure blockchain technology to enhance trust and reliability in the context of medical services.

7.3.3 Promoting Open Source Collaboration

- Make the system and smart contracts open source to encourage transparency and innovation.
- Host the project on GitHub to facilitate contributions and collaboration from a diverse community of developers.
- Cultivate a culture of shared knowledge and continuous improvement through open-source principles.

7.3.4 Enabling Seamless Integration with Organizational Partners

- Establish seamless integration with the Analysis Laboratory, allowing for efficient exchange of medical tests and radiology data.
- Integrate with the Hospital's system to provide doctors with access to relevant patient information.
- Design the system to accommodate future integrations with other organizations, ensuring scalability and adaptability.

Moving forward, "Rosheta" is poised to continue innovating and expanding its capabilities, ultimately revolutionizing the landscape of digital healthcare delivery.

7.4 Future Work

- Points 9,10 and 11 from the need to extend related work:
    1. There is a need to provide an Appointments Calendar for scheduling doctor appointments.
    2. There is a need to apply analysis and machine learning to data and give summaries to doctors which help in future research works.
    3. Provide a solution that will help in digitalization and automation of the diagnosis process By Doctor Y.

7.5 Conclusion

In this chapter, the Conclusion, contribution, and future work were introduced.
In the next chapter, we will show many useful appendices.

8 References

[1] AlmaLnews. alwatan article: number of hospitals and clinics in cairo. Last accessed: Jan. 28, 2024, 2024. Available online.

[2] Reinhold Haux. Health information systems - past, present, future. *International Journal of Medical Informatics*, 75(3-4):268–281, 2006.

[3] Kabiru Danladi Garba and Idris Yahaya. Significance and challenges of medical records: A systematic literature review. *Advances in Librarianship*, 9:26–31, 06 2018.

[4] Record Nations. Pros and cons of paper medical records, not specified.

[5] Faisal Reza, José Tomás Prieto, and Stephen Julien. Electronic health records: Origination, adoption, and progression. pages 183–201, 07 2020.

[6] Suzanna Schmeelk, Megha Kanabar, Kevin Peterson, and Jyotishman Pathak. Electronic health records and blockchain interoperability requirements: a scoping review. *JAMIA Open*, 5(3):ooac068, 07 2022.

[7] S. Rajput, A. Singh, S. Khurana, T. Bansal, and S. Shreshtha. Blockchain technology and cryptocurrencies. In *2019 Amity International Conference on Artificial Intelligence (AICAI)*, pages 909–912, 2019.

[8] Amos Kibet, Demeke Gebresenbet Bayou, and Rosanna Esquivel. Blockchain: It's structure, principles, applications and foreseen issues. In *Journal of Emerging Technologies and Innovative Research (JETIR)*, volume 6, 2019.

[9] Yan Zhuang, Chi-Ren Shyu, Shenda Hong, Pengfei Li, and Luxia Zhang. Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology. *Health Blockchain Journal*, 7(2):123–136, 2023.

[10] Nick Szabo. Smart contracts. *LOTwinterschool 2006*, 1994.

[11] IBM. Smart contracts - ibm. `https://www.ibm.com/topics/smart-contracts`.

[12] Encyclopaedia Britannica. How smart contracts work. `https://www.britannica.com/money/how-smart-contracts-work#ref356871`.

[13] Investopedia. Smart contracts - investopedia. `https://www.investopedia.com/terms/s/smart-contracts.asp#toc-smart-contract-uses`.

[14] Ethereum Foundation. Ethereum: A decentralized platform for applications. `https://ethereum.org/`, 2023.

[15] Ethereum Foundation. Introduction to ethereum. https://ethereum.org/en/developers/docs/intro-to-ethereum/.

[16] Ethereum Foundation. Accounts - ethereum developer documentation. https://ethereum.org/en/developers/docs/accounts/.

[17] Ethereum Foundation. Gas - ethereum developer documentation. https://ethereum.org/en/developers/docs/gas/.

[18] Ethereum Foundation. Smart contracts - ethereum developer documentation. https://ethereum.org/en/developers/docs/smart-contracts/.

[19] Christian Cachin. Architecture of the hyperledger blockchain fabric. *IBM Research - Zurich*, 2016.

[20] Hyperledger 2020-2023. Hyperledger fabric documentation. https://hyperledger-fabric.readthedocs.io/en/release-2.5/whatsnew.html.

[21] Hyperledger fabric ecosystem. https://wiki.hyperledger.org/display/fabric/Ecosystem. Accessed: June 20, 2024.

[22] Xun (Brian) Wu. *Hyperledger Cookbook: Over 40 recipes implementing the latest Hyperledger blockchain frameworks and tools*. Packt Publishing Ltd, 2019.

[23] Nick O'Connell and Ayman Nour. New personal data protection law in egypt. https://www.mondaq.com/data-protection/977748/new-personal-data-protection-law-in-egypt, 2020. Accessed: June 20, 2024.

[24] Álvaro Díaz and Héctor Kaschel. Scalable electronic health record management system using a dual-channel blockchain hyperledger fabric. *Systems*, 11(7):346, 2023.

[25] F. K. Nishi, M. Shams-E-Mofiz, M. M. Khan, A. Alsufyani, S. Bourouis, P. Gupta, and D. K. Saini. Electronic healthcare data record security using blockchain and smart contract. *IEEE Open Access*, 2022(7299185):1–7, May 29 2022.

[26] P. Chinnasamy, Ashwag Albakri, Mudassir Khan, A. Ambeth Raja, Ajmeera Kiran, and Jyothi Chinna Babu. Smart contract-enabled secure sharing of health data for a mobile cloud-based e-health system. *Applied Sciences*, 13(6), 2023.

[27] Harsha Aggarwal, Deo Vidyarthi, Arun Arora, Rahul Johari, and Deo Vidyarthi. Best: Blockchain-enabled secure technology in health care management system.

[28] Leila Ismail, Huned Materwala, and Youssef Sharaf. Blockhr – a blockchain-based healthcare records management framework: Performance evaluation and comparison with client/server architecture. pages 1–8, 2020.

[29] Burstiq health. https://burstiq.com/, [Accessed: 12/14/2023].

[30] Medicalchain. https://medicalchain.com/en/, [Accessed: 12/14/2023].

[31] Patientory. https://patientory.com/, [Accessed: 12/14/2023].

[32] Medibloc. https://medibloc.com/, [Accessed: 12/14/2023].

[33] Medrec. https://medrec-m.com/, [Accessed: 12/14/2023].

[34] A. Roehrs, C. A. da Costa, and R. da Rosa Righi. Omniphr: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, 71:70–81, 2017.

[35] Omar Reda Abo El-Yazed, Mohamed Hossam El-Ashry, Ahmed Samy Ahmed, Mark Adel Antoun, Ahmed Abdelhamid Ahmed, and AbouBakr Hussien Shahin. Doctor-y: Artificial intelligence assisted connection between patients and physicians. Graduation Project, 2023.

[36] Software Engineering Competence Center (SECC). *SPIG Product Suite Handbook V1.2, Software Process Improvement Guide (SPIG).* Information Technology Industry Development Agency (ITIDA), Ministry of Communications and Information Technology (MCIT), Giza, Egypt, 2010.

[37] Google. Flutter documentation. https://docs.flutter.dev/, [Accessed: 12/29/2023].

[38] Wikipedia contributors. Flutter (software). https://en.wikipedia.org/wiki/Flutter_(software), [Accessed: 12/29/2023].

[39] Node.js documentation. https://nodejs.org/docs/latest/api/, [Accessed: 12/29/2023].

[40] Wikipedia contributors. Node.js. https://en.wikipedia.org/wiki/Node.js, [Accessed: 12/29/2023].

[41] Wikipedia contributors. Express.js. https://en.wikipedia.org/wiki/Express.js, [Accessed: 12/29/2023].

[42] Mongodb official website. https://www.mongodb.com/, [Accessed: 5/21/2024].

[43] Wikipedia contributors. Mongodb. https://en.wikipedia.org/wiki/MongoDB, [Accessed: 5/21/2024].

[44] Hyperledger fabric documentation. https://hyperledger-fabric.readthedocs.io/en/release-2.5/, [Accessed: 12/29/2023].

[45] Amazon Web Services. What is hyperledger fabric?, [Accessed: 12/29/2023].

[46] Git documentation. https://git-scm.com/doc, [Accessed: 12/29/2023].

[47] Wikipedia contributors. Git. https://en.wikipedia.org/wiki/Git, [Accessed: 12/29/2023].

[48] P. Chinnasamy and P. Deepalakshmi. Improved key generation scheme of rsa (ikgsr) algorithm based on offline storage for cloud. In Elijah Blessing Rajsingh, Jey Veerasamy, Amir H. Alavi, and J. Dinesh Peter, editors, *Advances in Big Data and Cloud Computing*, pages 341–350, Singapore, 2018. Springer Singapore.

[49] Debendranath Das, Amudhan Muthaiah, and Sushmita Ruj. *Blockchain-Enabled Secure and Smart Healthcare System*, pages 97–109. 05 2022.

9 Appendix A : Research Papers Summaries

A.1: Scalable Electronic Health Record Management System Using a Dual-Channel Blockchain Hyperledger Fabric [24]

Authors: Álvaro Díaz , Héctor Kaschel.
Published in: July 2023
What is your take-away message from this paper ?
The paper presents scalable blockchain-based Electronic Health Record (EHR) management system that addresses scalability issues and enhances the security and privacy of patients' medical data.

What is the motivation for this work (both people's problem and technical problem), and its distillation into a research question? Why doesn't the people's problem have a trivial solution? What are the previous solutions and why are they inadequate?

The motivation for this research arises from two intertwined problems. The first is the people's problem, which pertains to the growing concerns over the security and privacy of sensitive personal data in the healthcare sector. The second is the technical problem, which involves finding a robust and reliable solution to address these concerns.

The research question distilled from these problems is: "How can blockchain technology be leveraged to enhance the privacy and security of sensitive personal data in healthcare applications?"

The people's problem does not have a trivial solution due to the complexity and sensitivity of the data involved. Healthcare data is not only personal but also highly confidential. Therefore, any solution must ensure the utmost security and privacy while still allowing for necessary access and use.

Previous solutions have attempted to address these issues, but they have proven inadequate due to various reasons. Traditional centralized data management systems are vulnerable to single-point failures and attacks. Moreover, they lack transparency, which is crucial for trust in healthcare applications.

Blockchain technology, with its decentralized, consensus-based approach, offers a promising alternative. Its key elements related to security and privacy, such as distributed consensus procedures and cryptographic techniques, make it a potential game-changer in addressing the privacy and security issues in healthcare applications. This research aims to delve deeper into these aspects, exploring their potential

and elucidating their workings in detail.

What is the methodology of the proposed solution (hypothesis, idea, design)?
The methodology of this paper is divided into four main steps as in **Figure 6** :

1. **Conceptualization**: A conceptual model for managing Electronic Health Records (EHR) using blockchain technology is initially developed. This model is designed with scalability in mind.
2. **Adaptation**: The model is then adapted to fit the Hyperledger Fabric blockchain platform. This involves aligning the features of the model with the components of the Hyperledger Fabric.
3. **Prototype Implementation**: Two test prototypes are created. The first one follows the traditional architecture of Hyperledger Fabric blockchain, while the second one incorporates the scalability features of the model.
4. **Performance Testing**: The performance of the model is tested. The Hyperledger Caliper tool is used to conduct two sets of tests: one on the traditional prototype and another on the prototype with the model's scalability features. The results are then compared and analyzed to evaluate the effectiveness of the model.

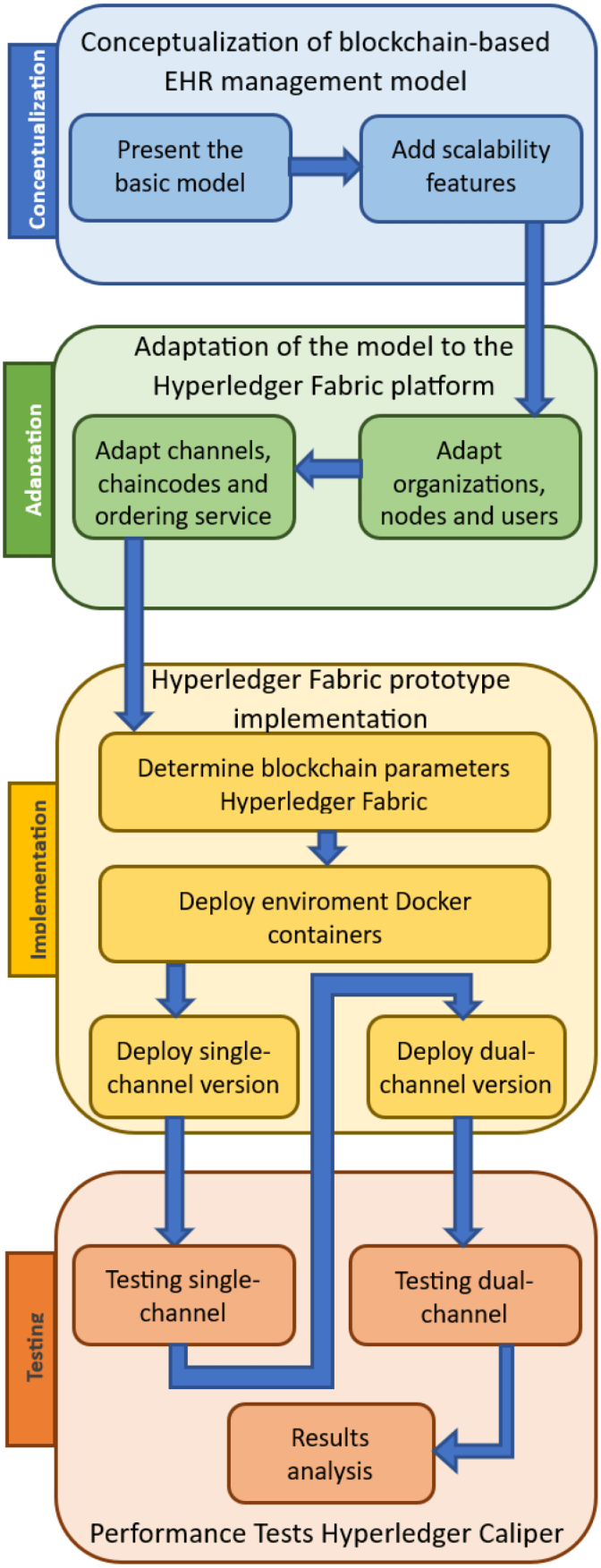

Figure 6: Summary diagram of the methodology of this paper.

Proposed Model:

Each organization interacts in a decentralized data system. For the scheme, they

implemented four organizations viz: Hospital, Laboratory, Research Center, and Health Insurance Provider. Each of these organizations has a generic character and does not represent a particular institution. Thus, each organization has different types of users: for the Hospital; the users are patients, doctors, nurses, and paramedics, among others. For the Laboratory, the users are laboratory technicians, radiologists, and biotechnologists, among others. For the Research Center, the users are scientific researchers and systems analysts. Finally, in the Health Insurance Provider, the users are consultants, vendors, and insurance administrators. A schematic of the proposed architecture is shown in **Figure** 7

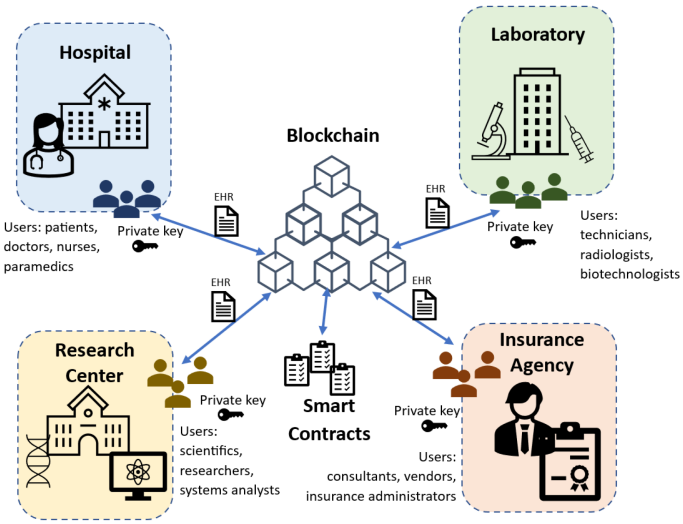

Figure 7: Scheme of the proposed architecture using four organizations: Hospital, Laboratory, Research Center, and Insurance Agency.

What is the author's evaluation of the solution? What logic, argument, evidence, artifacts (e.g., a proof-of-concept system), or experiments are presented in support of the idea?
The authors evaluated their solution by comparing the performance of a single-channel network with a dual-channel network in the Hyperledger Fabric blockchain platform. They used several parameters for this evaluation, including decentralization, security and privacy, latency, and scalability. The logic behind this comparison is to demonstrate the improvements brought about by their proposed dual-channel model. Evidence presented includes throughput parameters, latency times, and successful transaction probabilities. Two prototypes were created for this purpose: one following the traditional architecture of Hyperledger Fabric blockchain (single-channel), and the other incorporating the scalability features of their model (dual-channel)

What are the paper's contributions (author's and your opinion)? Ideas, methods, software, experimental results, experimental techniques...?
The key contribution of the authors is the demonstration of the significant advantages of a dual-channel network over a single-channel network, particularly in terms of throughput for both Create Rate and Query Rate rounds. This is evidenced by

the data presented in Figures 8 and 9.

In Figure 8, the throughput for the Create Rate round is compared between the single-channel and dual-channel networks. The dual-channel network shows a clear improvement in performance.

Similarly, in Figure9, the throughput for the Query Rate round is compared between the two types of networks. Again, the dual-channel network exhibits superior performance.

In summary, the authors have effectively proven that the use of a dual-channel network can lead to substantial enhancements in throughput for both Create Rate and Query Rate rounds. This finding is a significant contribution to the field.

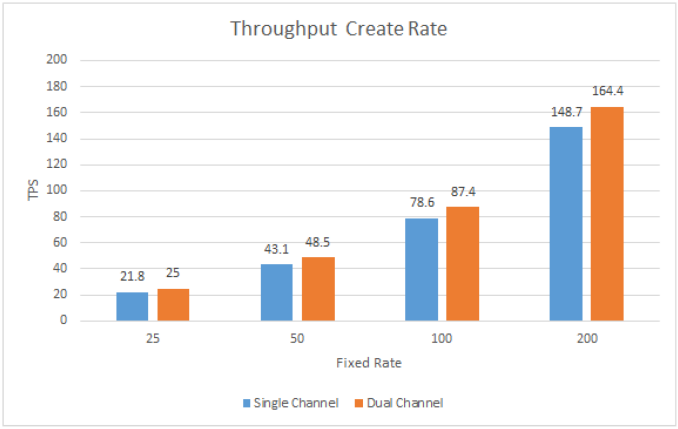

Figure 8: Create Rate round throughput, comparison between single channel and dual channel.

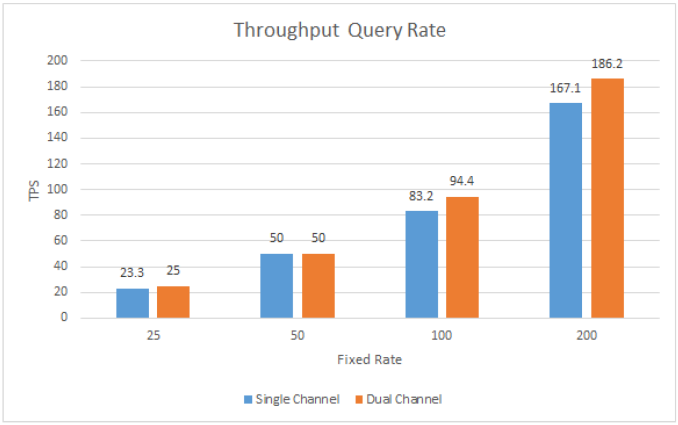

Figure 9: Query Rate round throughput, comparison between single channel and dual channel.

Finally, The performance improvements achieved with the dual-channel blockchain are present but relatively small, around 10% with a peak of 14.7%. For high transaction rates, the performance is limited by shared hardware resources, suggesting that distributing nodes across different machines could yield better results. For low transaction rates, significant improvements are observed, particularly in the Create Rate round. The dual-channel network also shows enhanced transaction effectiveness, with a success rate of 99.925% in the Query Rate rounds. This suggests that while the dual-channel network offers improvements, further scalability solutions

may be needed for optimal performance. **What are the future directions for this research (the author's and yours, perhaps driven by shortcomings or other critiques)?**

The future research directions include evaluating the influence of hardware capabilities on blockchain performance using a multi-host testing prototype. The authors also plan to enable more channels with more participating organizations to avoid isolation in the health system. They aim to address the problem of EHR management document storage in a Hyperledger Fabric scheme and intend to use real EHR datasets from open medical research repositories. Lastly, the implementation of a user-friendly interface is planned for easier interaction with real data.

A.2: Electronic Healthcare Data Record Security Using Blockchain and Smart Contract [25]

Authors: Farjana Khanam Nishi, Mahizebin Shams-E-Mofiz, Mohammad Monirujjaman Khan, Abdulmajeed Alsufyani, Sami Bourouis, Punit Gupta and Dinesh Kumar Saini

Published in: May 2022

What is your take-away message from this paper ?

Blockchain's decentralized nature and smart contracts offer potential solutions to the security challenges in healthcare data management.

What is the motivation for this work (both people's problem and technical problem), and its distillation into a research question? Why doesn't the people's problem have a trivial solution? What are the previous solutions and why are they inadequate?

The people problem in healthcare data management predominantly concerns two critical areas. Firstly, the issue of data privacy and security remains a prevalent challenge within healthcare systems. These systems often lack the robustness required to safeguard patient information, resulting in frequent breaches and compromises in patient confidentiality. Secondly, patients encounter obstacles in accessing and managing their medical records across various healthcare providers, highlighting concerns about data accessibility and control in the healthcare sector.

From a technical standpoint, existing healthcare data systems face challenges due to centralized data storage practices. Such centralized systems are prone to vulnerabilities, leaving them exposed to breaches and data theft, raising concerns about the overall security of patient information. Furthermore, the absence of user-friendly solutions in previous blockchain-based healthcare systems accentuates the need for more integrated, intuitive platforms that cater to the diverse needs of patients and healthcare providers.

At the core of this research inquiry is the exploration of whether a blockchain-based system can effectively rectify the deficiencies prevalent in healthcare data management. The research question centers on the potential of blockchain technology to address security, accessibility, and patient-controlled sharing within healthcare data. It seeks to strike a balance between stringent data security measures and the universal usability of the system, aiming to empower patients while ensuring the safeguarding of their data.

The non-trivial nature of this challenge arises from the complex intersection between stringent data security, universal data accessibility, and patient autonomy.

Balancing these critical aspects in healthcare data management poses a significant challenge. The technical solutions must navigate the delicate balance between high-security standards and user-friendly interfaces, particularly in a healthcare ecosystem where data sensitivity is paramount.

Previous attempts to resolve healthcare data management issues have often revolved around centralized data systems or relied on basic encryption methods. However, these solutions have demonstrated inadequacies. Centralized systems are vulnerable to single-point breaches, compromising entire databases, while basic encryption methods might not suffice against sophisticated cyber threats. Moreover, past solutions often overlooked the aspect of patient control, limiting accessibility and control over personal medical data. These deficiencies in prior solutions emphasize the urgency of exploring innovative approaches, such as blockchain integration with smart contracts, to establish a decentralized, secure, and patient-controlled healthcare data management system.

What is the proposed solution (hypothesis, idea, design)? Why is it believed it will work? How does it represent an improvement? How is the solution achieved?
The proposed solution integrates blockchain technology, particularly the Ethereum blockchain, and smart contracts into healthcare data management. This integration aims to create a secure, decentralized system that grants patients control over their medical records while ensuring accessibility and data integrity.

This solution leverages blockchain's decentralized nature to enhance security by eliminating single points of failure and employs smart contracts to automate access control, giving patients the authority to manage who can access their data. By integrating these technologies, the system intends to offer improved security, patient empowerment, and data integrity, marking a departure from the limitations of traditional centralized healthcare data systems.

What is the author's evaluation of the solution? What logic, argument, evidence, artifacts (e.g., a proof-of-concept system), or experiments are presented in support of the idea?
The evaluation is supported by several logical arguments and evidence presented throughout the paper:

1. **Logic and Argumentation**:The paper logically argues that traditional medical record-keeping methods are inefficient and lack proper structuring, leading to challenges in data transmission. It emphasizes the need for improved data management methods without compromising security or privacy.
2. **Blockchain Technology**: The author posits that blockchain technology, specif-

ically Ethereum-based smart contracts, can resolve issues related to data integrity, accessibility, accuracy, and security within healthcare systems. The immutability of the ledger, use of smart contracts for data modifications, and the decentralized nature of blockchain are highlighted as key advantages.

3. **System Architecture and Components**: The paper describes the proposed system's architecture, detailing components like Ethereum, IPFS, MetaMask, and other tools utilized. This description provides a theoretical framework for how the system is expected to function.The architecture in Figure 10

4. **Demonstration and Artifacts**: The paper includes visual aids (figures) showcasing the user interface of the proposed system, such as the homepage, admin panel, doctor's panel, and patient's panel. These visuals demonstrate how users interact with the system and manage medical records.

5. **Use Case Diagram and Flowcharts**: Use case diagrams and flowcharts are presented to illustrate the step-by-step processes within the system, such as adding doctors/patients, deleting users, uploading medical records, and system interaction.The use case digram in Figure 11

6. **Comparison with Existing Systems**: A comparative analysis is conducted, highlighting the strengths of the proposed system, particularly its security mechanisms and smart contract integration, in contrast to weaknesses observed in other studies or systems.

What is your analysis of the identified problem, idea and evaluation? Is this a good idea? What flaws do you perceive in the work? What are the most interesting or controversial ideas? For work that has practical implications, ask whether this will work, who would want it, what it will take to give it to them, and when might it become a reality?
The identified problem in the paper revolves around inefficiencies and security concerns in healthcare data management. The idea proposed involves leveraging blockchain to create a decentralized, secure system for managing medical records and transactions. The evaluation indicates a positive view, emphasizing the potential benefits of increased security and accessibility in healthcare data.

However, while the idea seems promising theoretically, its practical implementation raises several concerns. One major issue is the complexity of integrating blockchain into existing healthcare systems. Blockchain adoption in healthcare faces regulatory hurdles, interoperability challenges, and scalability issues. Additionally, the scalability of blockchain networks, especially in handling the massive volume of healthcare data, remains a significant concern.

The most interesting aspect is the proposition of using blockchain for data security

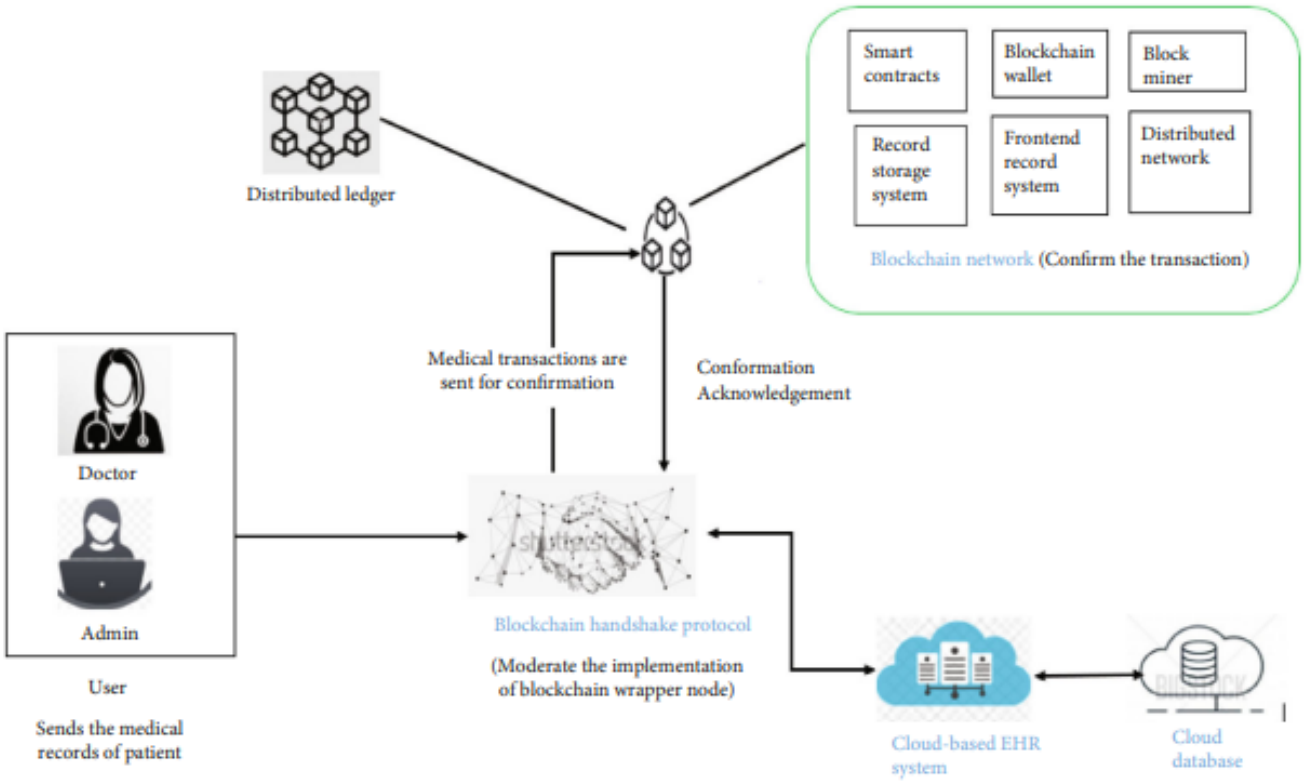

Figure 10: Block diagram of the blockchain-based EHR system

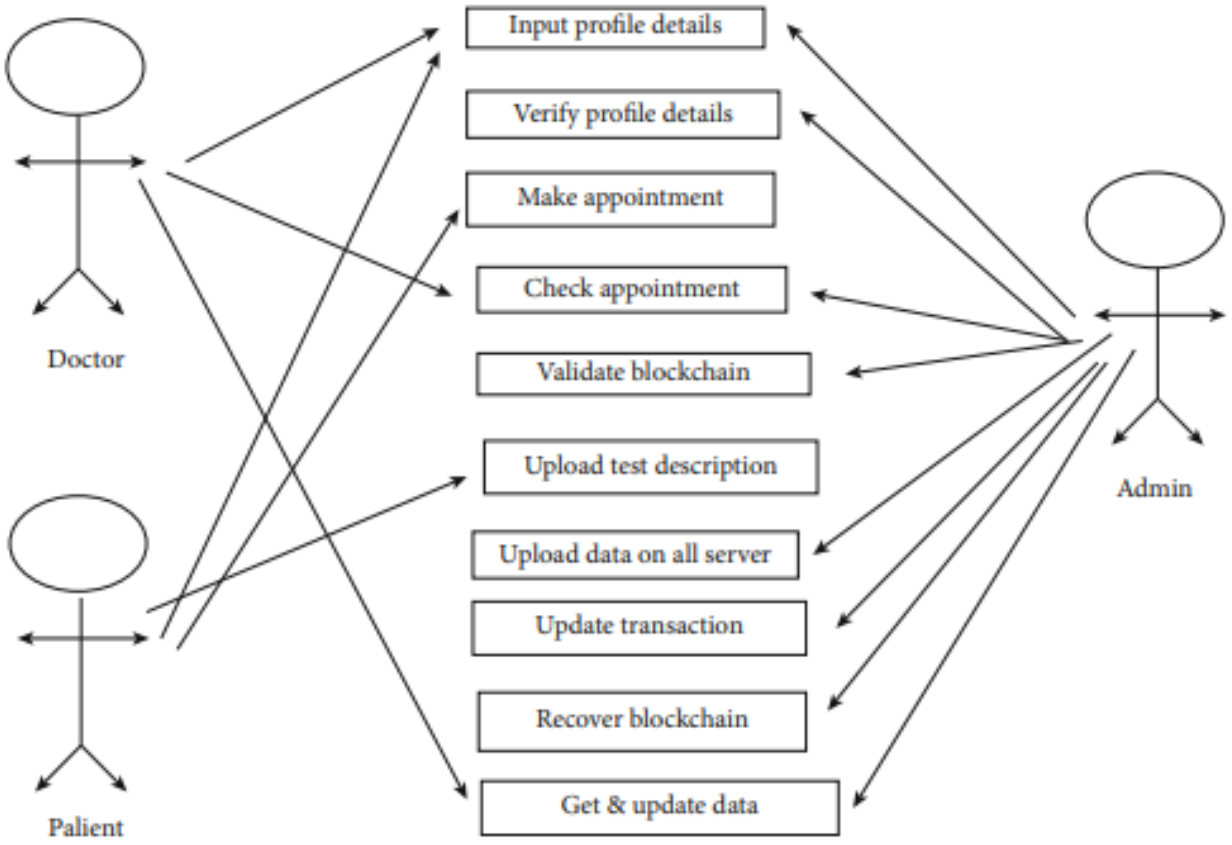

Figure 11: Use case diagram of the EHR system.

and patient-controlled access, which could revolutionize healthcare data management. Nevertheless, the controversial part lies in the practicality and feasibility of implementing such a system within the complex healthcare infrastructure.

For practical implications, the success of this idea depends on various factors, including regulatory acceptance, technological advancements to ensure scalability, interoperability with existing systems, and user acceptance within the healthcare ecosystem. It will require collaboration among healthcare institutions, technology providers, policymakers, and regulatory bodies. The timeline for its realization might span several years, considering the need for infrastructure development, regulatory frameworks, and widespread acceptance.

Overall, while the idea of using blockchain in healthcare holds promise, its practical implementation demands overcoming significant technical, regulatory, and practical hurdles before becoming a reality.

What are the paper's contributions (author's and your opinion)? Ideas, methods, software, experimental results, exper- imental techniques...?

1. **Idea and Conceptual Contribution**: The paper introduces the concept of utilizing blockchain technology in healthcare for secure, decentralized management of medical records. This idea represents a paradigm shift in how healthcare data could be managed, emphasizing patient-controlled access and increased security.
2. **Methodological Contribution**: It outlines the implementation of Ethereum-based smart contracts and the Interplanetary File System (IPFS) for storing and managing medical records securely. The proposed framework leverages various tools such as Ganache, MetaMask, Truffle, and Web3 to create a robust healthcare management system.
3. **Software and Technological Contribution**: The paper describes the use of specific software tools and languages, including Solidity, Node.js, React.js, and HTML/CSS for building the front-end and back-end infrastructure of the proposed healthcare management system.
4. **Experimental Techniques and Results**: The paper details the step-by-step process of the system, providing visual representations of the user interfaces, administrative functionalities, doctor's and patient's panels. These visual representations illustrate how the system operates and the functionalities available to different user roles.

5. **Evaluation and Analysis**: The authors evaluate the solution through a comprehensive examination of existing healthcare systems, discussing the limitations and potential of their proposed blockchain-based approach. They present arguments supporting the benefits of their solution, such as increased security, accessibility, and cost-effectiveness.

What are future directions for this research (author's and yours, perhaps driven by shortcomings or other critiques)?

Future directions for this research encompass various key aspects that aim to bridge existing gaps and enhance the applicability of blockchain-based healthcare data management systems. A crucial avenue involves real-world implementation, testing, and validation of the proposed system within healthcare institutions to ascertain its practicality and scalability in actual settings. Moreover, emphasizing interoperability standards and developing protocols for seamless data exchange between diverse healthcare systems emerges as a critical focus area for future exploration. Regulatory compliance remains imperative, necessitating a thorough understanding and adherence to healthcare data privacy regulations, such as HIPAA, ensuring legal compliance. Additionally, enhancing system scalability and performance to effectively handle the substantial volume of healthcare records and users, alongside fortifying security measures and encryption techniques to bolster patient data protection, stand as pivotal future research endeavors. Moreover, improving user experience through enhanced usability and providing comprehensive training for healthcare professionals and patients is essential. Lastly, there is a need to explore cost-effective implementation strategies and optimize resource utilization for sustainable and widespread adoption in healthcare settings.

What questions are you left with? What questions would you like to raise in an open discussion of the work (review interesting and controversial points, above)? What do you find difficult to understand? List as many as you can.

1. **Usability vs. Security**: How does the system balance usability for patients and healthcare providers with the need for robust security?
2. **Scalability Concerns**: In real-world scenarios with a vast number of healthcare records and users, how scalable is this system?
3. **Integration Challenges**: How easily can this blockchain-based system integrate with existing healthcare IT infrastructure?
4. **Legal and Ethical Implications**: What are the legal and ethical considerations when handling sensitive patient data on a blockchain?

5. **Practical Implementation**: What would it take for healthcare institutions to adopt and implement this system on a large scale?
6. **Regulatory Compliance**: Does the proposed system comply with existing healthcare data privacy regulations, and if not, what changes would be required?
7. **User Adoption**: How likely are patients and healthcare professionals to adopt and adapt to this new system, considering potential resistance to change?

A.3: Smart Contract-Enabled Secure Sharing of Health Data for a Mobile Cloud-Based E-Health System [26]

Authors: Chinnasamy, P. and Albakri, Ashwag and Khan, Mudassir and Raja, A. Ambeth and Kiran, Ajmeera and Babu, Jyothi Chinna.

Published in: March 2023

What is your take-away message from this paper ?

The paper proposes a novel approach for secure sharing of electronic health records (EHRs) using smart contracts and blockchain technology in a mobile cloud-based e-health system. The proposed system ensures data confidentiality, integrity, and availability, and provides a trusted access control mechanism for EHRs. The system was evaluated in various real-world scenarios, including IoTs and vehicular network virtualization, and was found to be effective in ensuring secure sharing of EHRs. The paper highlights the limitations of existing EHR sharing platforms and provides cost-effective solutions through a real-world simulation experiment. Overall, the proposed system is a milestone towards the efficient management of e-health information in portable computing and can be useful in many smart healthcare systems.

What is the motivation for this work (both people problem and technical problem), and its distillation into a research question? Why doesn't the people problem have a trivial solution? What are the previous solutions and why are they inadequate?

The motivation for this work stems from the increasing need for secure and efficient sharing of electronic health records (EHRs) in the context of mobile cloud-based e-health systems. This addresses both people and technical problems.

The people problem involves the need to ensure the privacy and security of sensitive health data while enabling efficient sharing among healthcare providers and patients. This is not a trivial problem because traditional methods of sharing healthcare data, especially in a mobile and cloud-based environment, often lack the necessary security measures to protect against unauthorized access and data breaches.

The technical problem involves the development of a system that can provide secure, reliable, and efficient access control for EHRs in a mobile cloud-based environment. This includes ensuring data confidentiality, integrity, and availability, as well as addressing the challenges of scalability and adaptability in diverse e-health scenarios.

The distillation of these problems into a research question could be: "How can we develop a secure and scalable access control mechanism for sharing electronic health records in a mobile cloud-based e-health system, ensuring data confidentiality, in-

tegrity, and availability, while addressing the limitations of existing EHR sharing platforms?"

Previous solutions for sharing EHRs have included traditional access control methods, public key infrastructure, and attribute-based encryption methods. However, these solutions have been inadequate in addressing the specific challenges of secure and efficient sharing of EHRs in a mobile cloud-based environment. They often lack the necessary scalability, adaptability, and comprehensive access control mechanisms to ensure the privacy and security of continuously produced data streams from sensors and monitoring devices in e-health applications. Additionally, existing methods have not fully leveraged the potential of blockchain technology and smart contracts to provide a robust and decentralized access control system for EHR sharing.

What is the proposed solution (hypothesis, idea, design)? Why is it believed it will work? How does it represent an improvement? How is the solution achieved?
The proposed solution in this paper is a secure and scalable access control mechanism for sharing electronic health records (EHRs) in a mobile cloud-based e-health system, using smart contracts and blockchain technology.

The hypothesis is that by leveraging the security and decentralization features of blockchain technology and smart contracts, it is possible to develop a robust and efficient access control mechanism for EHR sharing in a mobile cloud-based environment.

The proposed solution represents an improvement over existing methods by providing a comprehensive access control mechanism that ensures data confidentiality, integrity, and availability, while addressing the limitations of existing EHR sharing platforms. The proposed system is designed to be adaptable, scalable, and cost-effective, making it suitable for diverse e-health scenarios.

The solution is achieved through the following steps:

1. All data are collected from a local network channel and stored in a public cloud, where medical records are shared among authorized patients and healthcare providers.

2. Medical records are encoded with the public key of EHR management before being uploaded to decentralized cloud services based on the proposed architecture.

3. To receive data from the cloud, recipients must have access to the e-health owner's secret key to decode original information.

4. Smart contracts enforce an access control policy designed to restrict data access across untrusted parties, detect unauthorized entry into EHR stores, and enable healthcare data authenticity and monitoring.

5. The proposed system is evaluated in various real-world scenarios, including IoTs and vehicular network virtualization, and is found to be effective in ensuring secure sharing of EHRs.

Overall, the proposed solution provides a secure and efficient access control mechanism for EHR sharing in a mobile cloud-based e-health system, addressing the limitations of existing methods and leveraging the potential of blockchain technology and smart contracts.

What is the author's evaluation of the solution? What logic, argument, evidence, artifacts (e.g., a proof-of-concept system), or experiments are presented in support of the idea?
The authors evaluate the proposed solution through a real-world simulation experiment and provide a comprehensive assessment of the system's effectiveness. They present several logical arguments, evidence, and artifacts to support the idea of the proposed solution.

The authors argue that the proposed solution provides a reliable access control system that relies on smart contracts to regulate access rights and ensure efficient and reliable EHR information exchange. They emphasize the benefits of using blockchain technology and smart contracts to address the limitations of existing EHR sharing platforms and provide cost-effective solutions.

Evidence and Artifacts:

1. **Real-World Simulation Experiment:** Figure 12 depicts hospital information system scenario in which users such as patients, insurance companies, government agencies, and smart devices exchange data. IKGSR key generation, which produces the key pairs, initiates a sample set of circumstances workflow. Each smart gadget sends its attributes to the key generation authorities to register. After authentication, IKGSR sends the relevant device the Public Key. The device can use this key to generate the access code and encode its contents using the IKGSR encoding function using a blockchain-based smart contract. The medical supplier receives the uploaded encrypted files and access key. At that moment, the patients or smart devices send a query to HIS, and HIS responds by sending the patients or smart devices encrypted information and an authentication key. Patients or smart devices must finish the decoding procedure in order to access the encrypted message. The steps in deciphering

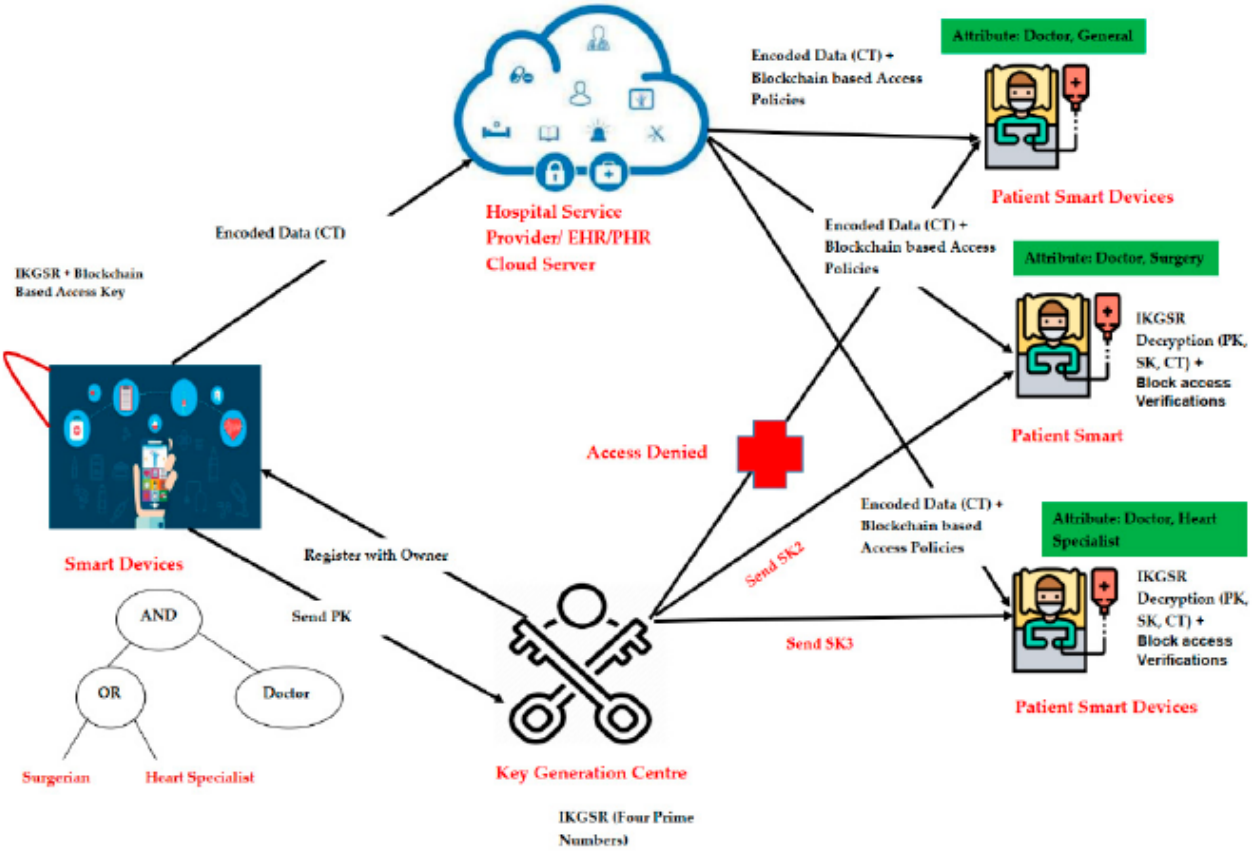

Figure 12: Application Scenario of the Proposed Method

are comparing the access key, trying to match the characteristics of the system administrator, and confirming the name of the system administrator. The adversaries or users won't be able to access the actual data of the owner when any of the three requirements are not met.

2. **Performance Evaluation:** The performance of the proposed framework is evaluated based on two criteria: the average time required to process the user's requests on the cloud and the time required to access the users' data. The average time required to evaluate several access user requests in the cloud was calculated (Figure 13). Compared to the approach without an authentication mechanism, our proposed system, which encompasses access control on smart contracts, takes longer to execute service requests. The time spent on identity management and authorization confirmation was added to this cost. However, the increased cost was approximately 5 s in the worst-case scenario—50 queries. Thus, it is considered to be minimal and appropriate for real-world situations. This result demonstrates the compact architecture of the proposed model for user authentication and authorization management.

   In addition, they demonstrate the capability of our EHR distribution system through the computational complexity of acquiring EHRs for the IPFS blockchain cloud storage (Figure 14).

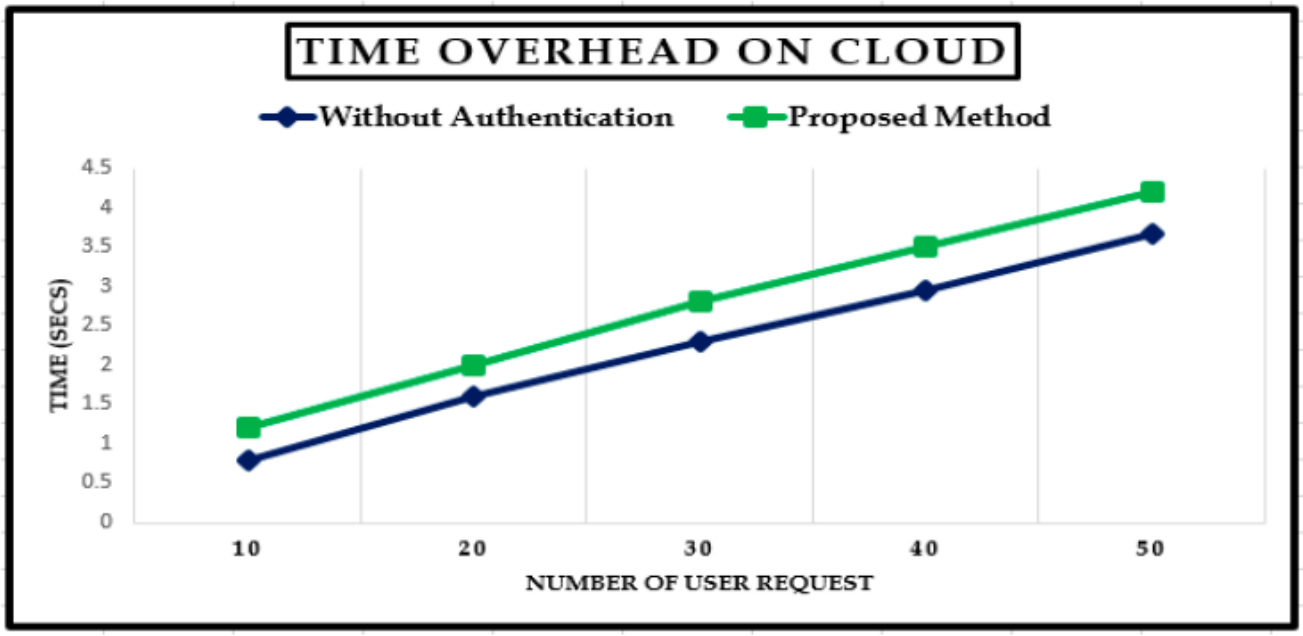

Figure 13: Average Time Overhead Based on the Number of User Requests.

They have already introduced the IKGSR[48] algorithm to enhance the security of asymmetric algorithms in cloud environments. In the proposed environment, They tested IKGSR against the traditional RSA algorithm. Figure 15 and Figure 16 clearly show that IKGSR requires more time to encode and decode input health data. However, the IKGSR algorithm offers high security as well as security against chosen ciphertext and timing attacks, as shown in[48].

3. **Security Evaluation:** Security is a major concern when implementing healthcare applications using various technologies; where sensitive data are protected from unauthorized access, the integrity of the data is enhanced, and the privacy of the users is enhanced. These assertions were used to demonstrate the trustworthiness of the proposed approach. A security analysis of the proposed framework is conducted using different attack situations. In addition, the advanced features of the suggested data exchange method are addressed to emphasize the utility and practicality of our approach.
Theorem 1. If an adversary has access to information in the cloud platform without permission granted by the EHR administrator, retrieving and reading health information through our systems is exceptionally difficult.
Proof. All health records were encoded with the public key of EHR management before being uploaded to decentralized cloud services based on our proposed architecture. To receive data from the cloud, recipients must have access to the e-health owner's secret key to decode original information. This secret key is unique, and only the EHR management can access it. Consequently, guessing the secret key to decode and acquire information in cloud storage is extremely difficult for an adversary.

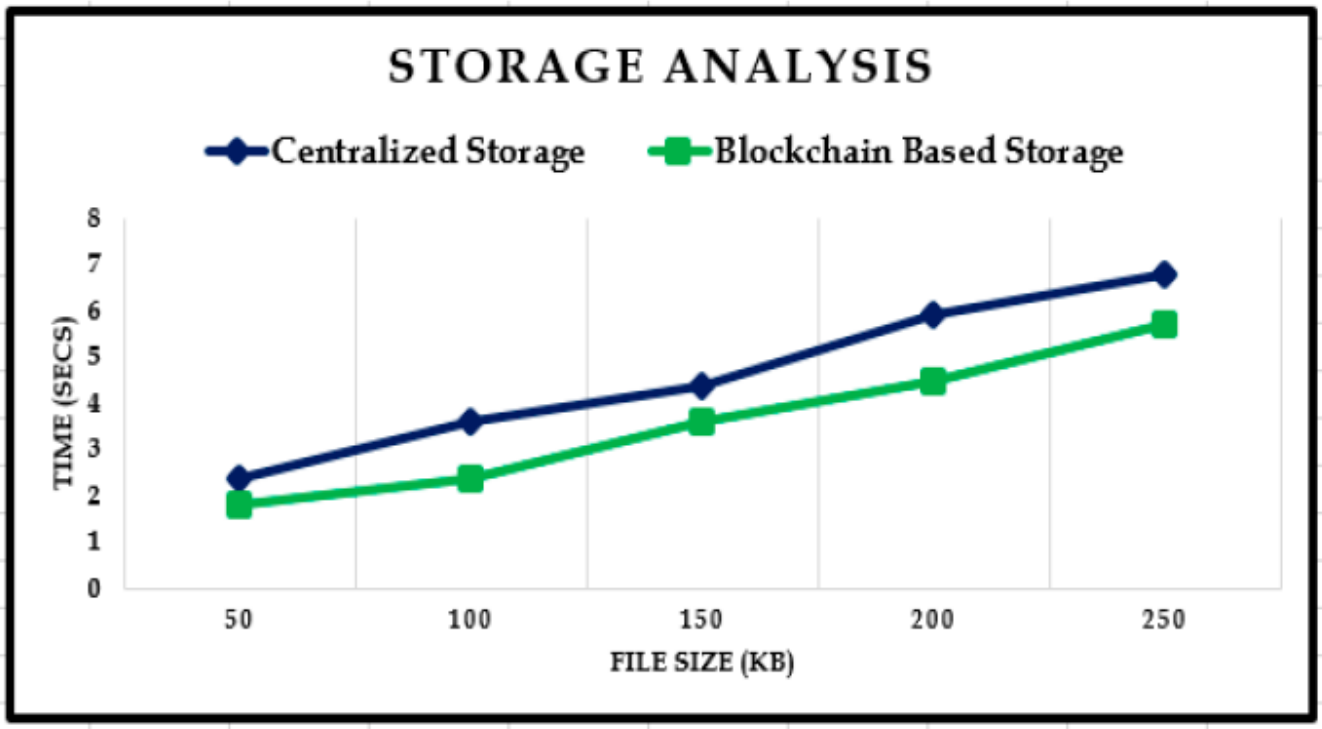

Figure 14: Time Required to Access the Data on the Cloud versus the Blockchain.

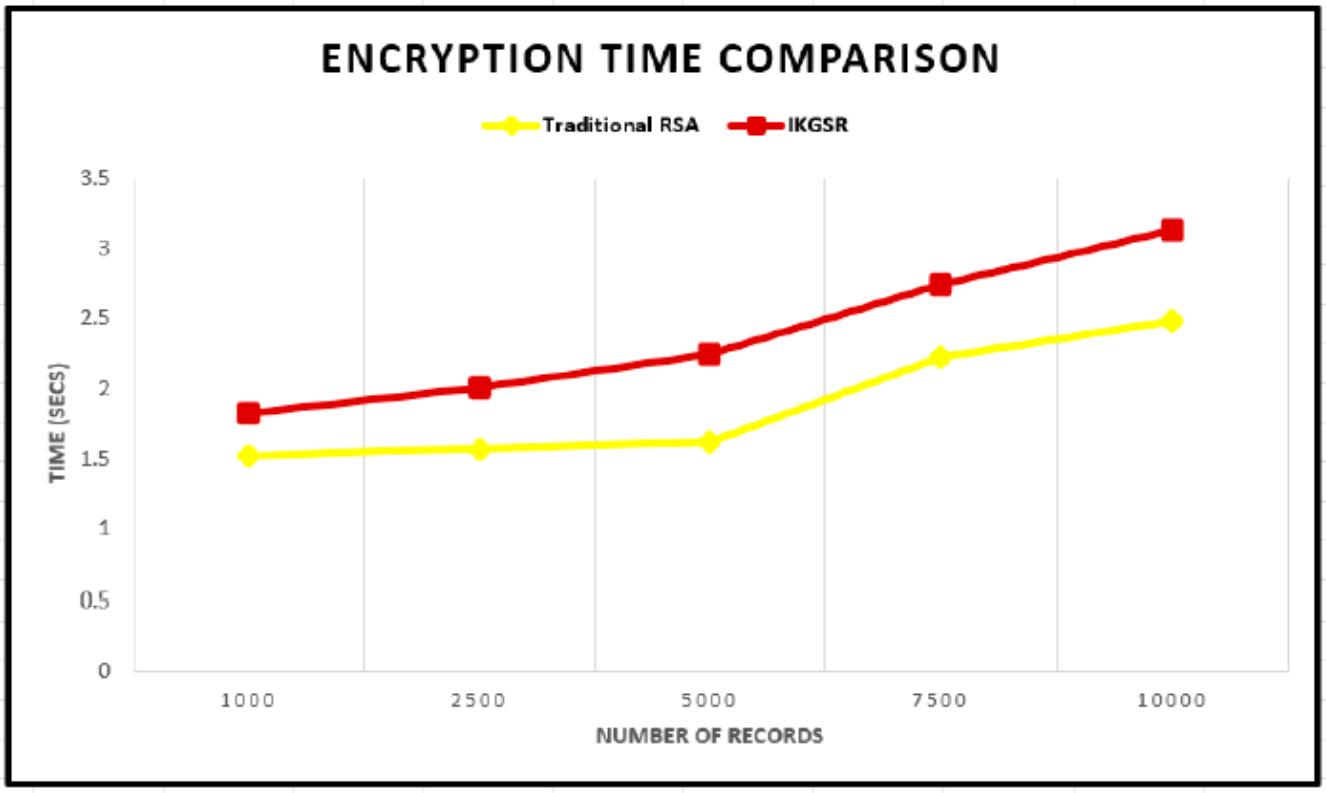

Figure 15: Encryption Time Comparison against Traditional RSA.

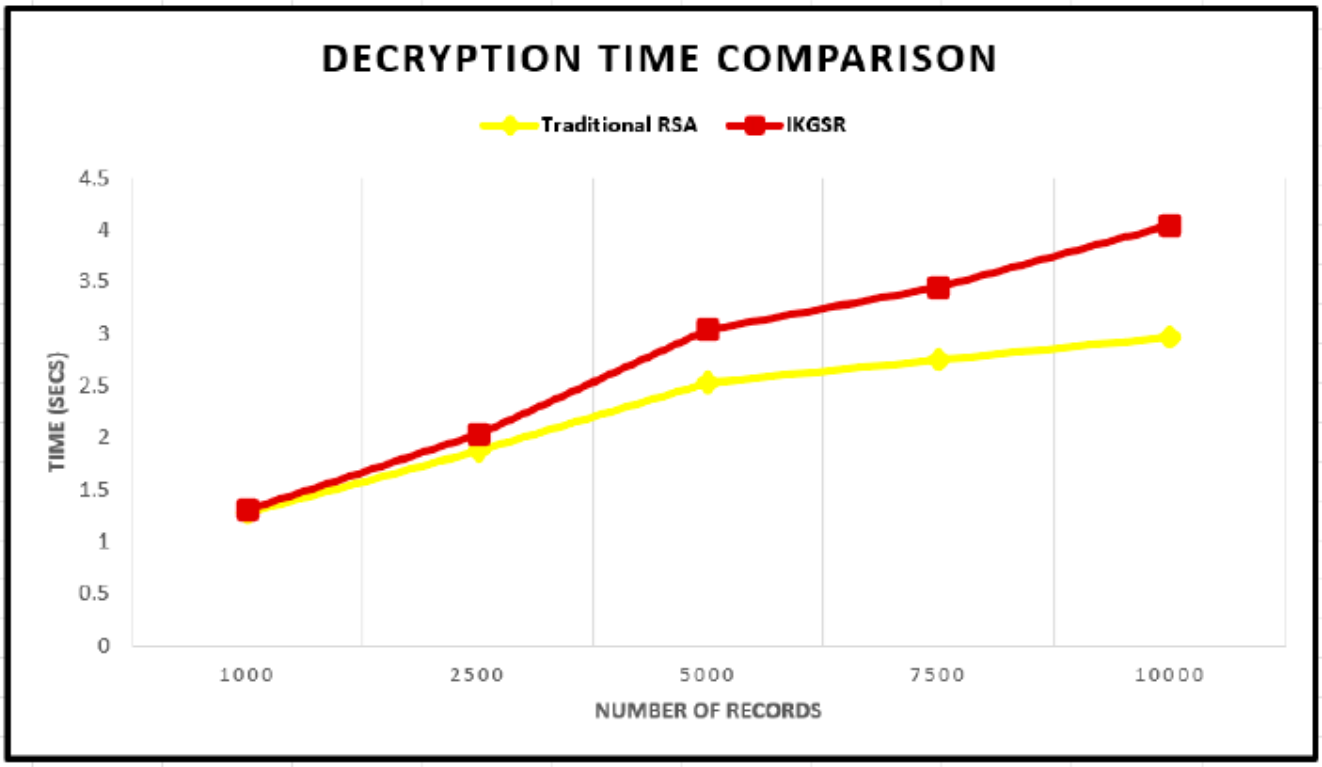

Figure 16: Decryption Time Comparison against Traditional RSA.

Theorem 2. Assume that an attacker can request cloud e-healthcare data through suspicious transactions. It is difficult for an attacker to gain authorization by tampering with the access control architecture.

Proof. To demand an approved transaction, a mobile node might need a private key (SK), public key (PK), and request ID, which are required to authenticate the transaction when it is sent to cloud services using the authorized (Tx) and SignSK syntax (rawTx PK, requestID, and timestamp). Only the user's public key is accessible to many individuals throughout the blockchain network, whereas the user's secret key is accessible only to the owner/user. Consequently, an attacker cannot authenticate transactions for database access using such a secret key. Additionally, because miners would remove any erroneous records from the Ethereum blockchain, the access management system would be impervious to any potential dangers.

Overall, the authors provide a robust evaluation of the proposed solution, supported by real-world simulation experiments, security analyses and performance evaluations.

What is your analysis of the identied problem, idea and evaluation? Is this a good idea? What flaws do you perceive in the work? What are the most interesting or controversial ideas? For work that has practical implications, ask whether this will work, who would want it, what it will

take to give it to them, and when might it become a reality?
The identified problem of secure and efficient access control for EHR sharing in mobile cloud-based e-health systems is a critical issue in the healthcare domain. The idea of utilizing blockchain technology and smart contracts to address this problem is innovative and has the potential to offer significant benefits in terms of data security, integrity, and accessibility. The evaluation presented in the paper provides a comprehensive assessment of the proposed solution, including real-world simulation experiments, security analyses, and performance evaluations, which adds credibility to the proposed approach.

The use of blockchain technology and smart contracts to enhance access control and secure EHR sharing in e-health applications is a promising idea. By leveraging the immutability and decentralized nature of blockchain, along with the programmable logic of smart contracts, the proposed solution aims to address the challenges associated with traditional access control methods and data sharing in healthcare systems.

One potential flaw in the work is the assumption of ubiquitous access to smartphones or portable devices, which may not be practical in all healthcare settings. Additionally, the complexity and resource requirements of implementing blockchain-based solutions may pose challenges, particularly in resource-constrained environments. Furthermore, the scalability and interoperability of the proposed system with existing healthcare infrastructure and standards may need further consideration.

The use of smart contracts to enforce access control policies and ensure data authenticity and monitoring is an interesting and innovative approach. The integration of blockchain technology and smart contracts in e-health applications presents a novel way to address security and privacy concerns in data sharing.

The proposed solution has practical implications for healthcare organizations, providers, and patients who require secure and efficient EHR sharing mechanisms. If successfully implemented, it could offer improved data security, integrity, and accessibility in e-health applications. However, the practical implementation of such a system would require collaboration between technology providers, healthcare organizations, and regulatory bodies to ensure compliance with data privacy and security regulations.

The feasibility and widespread adoption of the proposed solution will depend on various factors, including technological maturity, regulatory considerations, and the willingness of stakeholders to embrace blockchain-based solutions. Further research, pilot studies, and collaboration with industry partners will be essential to validate the practicality and effectiveness of the proposed system. The timeline for the re-

alization of such a solution will depend on the pace of technological advancements, regulatory frameworks, and industry readiness to adopt innovative approaches to data security and sharing in healthcare.

What are the paper's contributions (author's and your opinion)? Ideas, methods, software, experimental results, experimental techniques...?

1. **Idea and Conceptual Contribution:**
   (a) The paper propose a trustworthy access control system using smart contracts and blockchain technology for secure sharing of electronic health records (EHRs) in mobile cloud-based e-health systems.

   (b) Integration of blockchain technology and smart contracts to address the limitations of existing EHR sharing platforms, focusing on data confidentiality, integrity, and accessibility in e-health applications.

2. **Methodological Contribution:**
   (a) Utilization of smart contracts and blockchain technology to establish a secure access control system for sharing EHRs among patients and healthcare providers.

   (b) Real-world simulation experiment to evaluate the effectiveness of the proposed solution, providing practical insights into the performance and feasibility of the system in a simulated environment.

   (c) Security analyses and assessments of the proposed system to demonstrate its benefits over existing alternatives, emphasizing the potential to enhance data security in e-health applications.

3. **Software and Technological Contribution:**
   (a) Implementation of an Ethereum blockchain on the AWS cloud to evaluate the effectiveness of the proposed solution.

   (b) Creation of a mobile application interface to enable healthcare organizations to interact with EHR-centralized repositories through the proposed system.

4. **Experimental Techniques and Results:**

   (a) The paper employs a real-world simulation experiment to evaluate the proposed system, providing practical insights into its performance and feasibility in a simulated environment.

   (b) The experimental results demonstrate the effectiveness of the proposed system in providing secure and efficient access control for sharing EHRs in mobile cloud-based e-health systems.

5. **Evaluation and Analysis:** The evaluation and analysis in the paper provide a comprehensive assessment of the proposed system's performance, security features, and technological contributions. These analyses contribute to the validation and practical implications of the proposed system for secure data sharing in e-health applications.

What are future directions for this research (author's and yours, perhaps driven by shortcomings or other critiques)?
The future directions for this research, as suggested by the authors and potential additional considerations, could include the following:

1. **Scalability and Interoperability:** Future research could focus on enhancing the scalability and interoperability of the proposed system to accommodate a larger volume of electronic health records (EHRs) and ensure seamless integration with existing healthcare information systems. This could involve exploring interoperability standards and protocols for secure data exchange across diverse healthcare platforms.

2. **Privacy-Preserving Mechanisms:** Further investigation into privacy-preserving mechanisms within the proposed system could be valuable. This could involve exploring advanced cryptographic techniques or privacy-enhancing technologies to strengthen the protection of sensitive health information while maintaining data accessibility for authorized users.

3. **Regulatory Compliance and Governance:** Future research could address the regulatory compliance and governance aspects of the proposed system, considering the evolving landscape of healthcare data regulations and standards. This may involve aligning the system with relevant data protection regulations such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States or the General Data Protection Regulation (GDPR) in the European Union.

4. **Usability and User Experience:** Consideration of the usability and user experience aspects of the proposed system could be a focus for future research.

This may involve conducting user studies and incorporating user feedback to optimize the system's interface, accessibility, and overall user experience for both healthcare providers and patients.

5. **Integration with Emerging Technologies:** Exploring the integration of emerging technologies, such as artificial intelligence (AI) and Internet of Things (IoT), with the proposed system could be a promising avenue for future research. This could enable advanced analytics, predictive modeling, and real-time health monitoring capabilities within the secure EHR sharing framework.
6. **Ethical and Societal Implications:** Future research could delve into the ethical and societal implications of implementing the proposed system, considering factors such as data ownership, consent management, and the impact on patient-provider relationships. This could involve interdisciplinary collaboration with experts in bioethics, law, and social sciences.

These future directions aim to address potential shortcomings, enhance the robustness of the proposed system, and align with evolving healthcare needs and technological advancements.

What questions are you left with? What questions would you like to raise in an open discussion of the work (review interesting and controversial points, above)? What do you find difficult to understand? List as many as you can.

1. **Data Accuracy:** How does the proposed system ensure the accuracy and completeness of EHRs, particularly in cases where data may be incomplete or inconsistent across different healthcare providers?
2. **Data Integrity and Auditability:** How does the system ensure the integrity and auditability of EHRs, particularly in cases where the immutability of blockchain records may conflict with the need for data correction or updates?
3. **Potential Risks of Attacks:** How does the proposed system address the potential risks of data breaches or cyber attacks, particularly in cases where hackers may attempt to exploit vulnerabilities in the blockchain or smart contract components of the system?
4. **Potential Ethics:** How does the proposed system address the potential ethical and societal implications of EHR sharing, particularly in cases where sensitive health information may be used for research or other purposes without patients' explicit consent?
5. **Potential Barriers of New Technology:** How does the proposed system address the potential challenges of user adoption and acceptance, particularly

in cases where healthcare providers or patients may be hesitant to adopt new technologies or change established workflows?

6. **Potential Limitations and Trade-Offs:** What are the potential limitations or trade-offs associated with the proposed system, and how can these be mitigated to ensure a balanced approach to secure EHR sharing?

A.4: BlockHR – A Blockchain-based Healthcare Records Management Framework: Performance Evaluation and Comparison with Client/Server Architectur [28]

Authors: Leila Ismail, Huned Materwala and Youssef Sharaf

Published in: October 2020

What is your take-away message from this paper ?
Performance Evaluation and Comparison with Client/Server Architecture" is the proposal and evaluation of BlockHR, a blockchain-based framework for managing healthcare records. The paper highlights the advantages of using blockchain technology in healthcare, such as improved security, real-time data access, resistance to data fraud, and accurate patient care. It also discusses the limitations of the traditional client-server architecture for managing Electronic Health Records (EHRs) and compares the performance of BlockHR with the client-server approach. The authors emphasize the need for real implementation of the framework to extensively evaluate its security, privacy, and performance. Overall, the paper contributes to the growing body of research on blockchain applications in healthcare and provides insights into the potential benefits of blockchain-based healthcare record management systems.

What is the motivation for this work (both people problem and technical problem), and its distillation into a research question? Why doesn't the people problem have a trivial solution? What are the previous solutions and why are they inadequate?
The motivation for this work is the need for accurate, cost-efficient, and patient-centric healthcare records management. The traditional client-server approach suffers from several issues, including a single point of failure, data fragmentation, vulnerability, security, and privacy. These issues can lead to compromised patient data and inaccurate diagnoses, which can have severe consequences for patient health.
The technical problem addressed in this work is to propose a blockchain-based healthcare records management framework that addresses the limitations of the client-server approach. The proposed framework, BlockHR, aims to provide a secure, transparent, and efficient way of managing healthcare records across different hospitals and medical clinics.
The people problem is that patients and healthcare providers need a reliable and secure way of managing healthcare records that ensures privacy, security, and accuracy. The technical problem is to design a system that can address these needs while also being efficient and scalable.
Previous solutions, such as the client-server approach and cloud-based systems, have limitations in terms of security, privacy, and scalability. The client-server approach

suffers from a single point of failure, data fragmentation, and vulnerability, while cloud-based systems can be expensive and may not provide the necessary level of security and privacy.

What is the proposed solution (hypothesis, idea, design)? Why is it believed it will work? How does it represent an improvement? How is the solution achieved?

The proposed solution in this work is the development of BlockHR, a blockchain-based healthcare records management framework. The hypothesis is that by leveraging blockchain technology, it is possible to address the limitations of the traditional client-server approach and provide a more secure, transparent, and efficient system for managing healthcare records. It is believed that BlockHR will work due to the inherent features of blockchain technology, such as immutability, security, privacy, and data replication. By using a private blockchain network, BlockHR aims to prevent unauthorized and malicious access to healthcare records, which is crucial in the healthcare domain. The framework also incorporates a prediction tool that allows network participants and external users to predict their risk of developing a disease based on their health and lifestyle data, thus enabling better prognosis and diagnosis.

BlockHR represents an improvement over the client-server approach by addressing the issues of single point of failure, data stewardship, data fragmentation, vulnerability, security, and privacy. It also aims to provide real-time data access, resistance to data fraud, and accurate patient care.

The solution is achieved by developing a private blockchain network that connects different hospitals, patients, and healthcare providers. Each hospital maintains a copy of the ledger, and participants such as doctors and pharmacists act as full nodes, sending validated transactions to an administrator acting as a mining node. Patients in the network can upload and query their medical data, and the framework includes a prediction tool for disease risk assessment.

Overall, the proposed solution leverages the features of blockchain technology to provide a more secure, transparent, and efficient system for managing healthcare records, thus representing an improvement over traditional client-server approaches.

What is the author's evaluation of the solution? What logic, argument, evidence, artifacts (e.g., a proof-of-concept system), or experiments are presented in support of the idea?

The authors evaluate the proposed solution, BlockHR, by comparing its performance with the traditional client-server approach. They present evidence in the form of experimental results to support the effectiveness of BlockHR in addressing the identified problems in healthcare records management. The evaluation includes a comparison of execution times for data write and read operations between the client-

server approach and BlockHR. The experimental results demonstrate that while the client-server approach takes less execution time for recording medical data, BlockHR outperforms in terms of execution time for data access, being 20 times faster compared to the client-server approach for data read operations. This evidence supports the argument that BlockHR offers improved efficiency and real-time data access for healthcare records management.
The logic and argumentation presented in the paper are based on the inherent features of blockchain technology, such as immutability, security, and data replication, which are leveraged to address the limitations of the client-server approach. Additionally, the incorporation of a prediction tool for disease risk assessment based on health and lifestyle data adds further support to the effectiveness of the proposed solution.
While the paper does not explicitly mention the development of a proof-of-concept system or specific artifacts, the experimental results and performance evaluation serve as evidence of the feasibility and potential benefits of implementing BlockHR in real-world healthcare settings.

What is your analysis of the identied problem, idea and evaluation? Is this a good idea? What flaws do you perceive in the work? What are the most interesting or controversial ideas? For work that has practical implications, ask whether this will work, who would want it, what it will take to give it to them, and when might it become a reality?
The identified problem of healthcare records management, particularly the limitations of the traditional client-server approach, is well-addressed in this work. The idea of developing a blockchain-based framework, BlockHR, to improve the security, privacy, and efficiency of managing healthcare records is a promising one. The evaluation of the proposed framework provides valuable insights into its performance compared to the client-server approach, particularly in terms of execution time for data write and read operations.
While the idea of BlockHR is compelling, there are some potential flaws or limitations in the work. One aspect that could be further explored is the scalability of the proposed framework, especially as the number of medical records and network participants increases. Additionally, the practical implementation and real-world deployment of BlockHR would be a crucial next step to assess its effectiveness in a live healthcare environment.
One of the most interesting and potentially controversial ideas presented in the work is the use of blockchain technology in healthcare for data management and prediction tools. The incorporation of a prediction tool for disease risk assessment based on health and lifestyle data adds an innovative dimension to the framework.
In terms of practical implications, the question of whether BlockHR will work in real healthcare settings is important. Stakeholders such as healthcare providers, pa-

tients, and regulatory bodies would be interested in a secure and efficient healthcare records management system. To bring this framework to fruition, it would require collaboration with healthcare institutions, regulatory compliance, and addressing potential privacy and data security concerns.

What are the paper's contributions (author's and your opinion)? Ideas, methods, software, experimental results, experimental techniques...?
The paper's contributions include:

1. The proposal of BlockHR, a blockchain-based healthcare records management framework that addresses the limitations of the traditional client-server approach.
2. The evaluation of BlockHR's performance compared to the client-server approach in terms of execution time for data write and read operations.
3. The incorporation of a prediction tool for disease risk assessment based on health and lifestyle data.
4. The analysis of the effectiveness of BlockHR in providing security and privacy against the threats prevailing in the client-server approach.
5. The comparison of the proposed framework with the traditional client-server approach in terms of security, privacy, and efficiency.

In my opinion, the paper's contributions are significant, particularly in the context of healthcare records management. The proposal of BlockHR as a blockchain-based solution to address the limitations of the client-server approach is a novel and promising idea. The incorporation of a prediction tool for disease risk assessment adds further value to the proposed framework.
The experimental results and performance evaluation presented in the paper provide evidence of the feasibility and potential benefits of implementing BlockHR in real-world healthcare settings. The comparison with the traditional client-server approach highlights the advantages of using blockchain technology for healthcare records management.

What are future directions for this research (author's and yours, perhaps driven by shortcomings or other critiques)?
The future directions for this research, as identified by the authors and potential additional considerations, may include:

1. Real-world Implementation: The practical implementation of BlockHR in a live healthcare environment would be a crucial next step to assess its effectiveness and feasibility in addressing the identified limitations of the traditional client-server approach.

2. Scalability and Performance: Further research could focus on evaluating the scalability of BlockHR, especially as the number of medical records and network participants increases. Additionally, exploring methods to optimize the performance of the blockchain network for large-scale healthcare applications would be valuable.

What questions are you left with? What questions would you like to raise in an open discussion of the work (review interesting and controversial points, above)? What do you find difficult to understand? List as many as you can.
The questions which i would like to raise in an open discussion of the work are:

1. How can the proposed BlockHR framework be integrated with existing healthcare systems and electronic health record (EHR) platforms?

2. What are the potential ethical implications of using a blockchain-based healthcare records management framework, particularly in terms of data privacy and security?

And i can't understand clearly how can patient upload the data monitored and recorded by the sensor and medical devices attached ?

A.5: Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology [9]

Authors: Yan Zhuang, Chi-Ren Shyu, Shenda Hong, Pengfei Li and Luxia Zhang.

Published in: May 2023

What is your take-away message from this paper? The paper presents a novel approach to patient tokenization in healthcare using Non-Fungible Tokens (NFTs) and Self-Sovereign Identity (SSI) on a blockchain architecture. The proposed solution aims to enhance data security and patient control over data sharing.

What is the motivation for this work (both people problem and technical problem), and its distillation into a research question? Why doesn't the people problem have a trivial solution? What are the previous solutions and why are they inadequate?
The motivation stems from the need to protect patient privacy and confidentiality in healthcare, especially with the increasing volume and variety of data sources. The problem doesn't have a trivial solution due to the complexity of securely and anonymously linking data from disparate sources at the patient level. Previous solutions, such as the master patient index used in Health Information Exchange (HIE), have been inadequate due to concerns about data breaches and limitations in patient control over data sharing.

What is the proposed solution (hypothesis, idea, design)? Why is it believed it will work? How does it represent an improvement? How is the solution achieved? What is the author's evaluation of the solution? What logic, argument, evidence, artifacts (e.g., a proof-of-concept system), or experiments are presented in support of the idea?
The proposed solution introduces a novel approach to healthcare information exchange (HIE) authentication using Non-Fungible Tokens (NFTs) built on the Quorum blockchain. The key components of the system include three types of nodes (light nodes, full nodes, and archive nodes), each serving specific functions in the blockchain network. The system design comprises four modules: Creation, Linkage, Authentication, and Exchange as shown Figure 17. These modules collectively aim to address the challenges in patient identification, secure data sharing, and efficient HIE.

The hypothesis behind the proposed solution is that leveraging NFTs on a blockchain can provide a secure and decentralized method for patient identification, data sharing, and authentication in HIE. The adoption of the Quorum blockchain, with its Raft-based consensus mechanism, is believed to enhance scalability and efficiency in comparison to traditional blockchains.

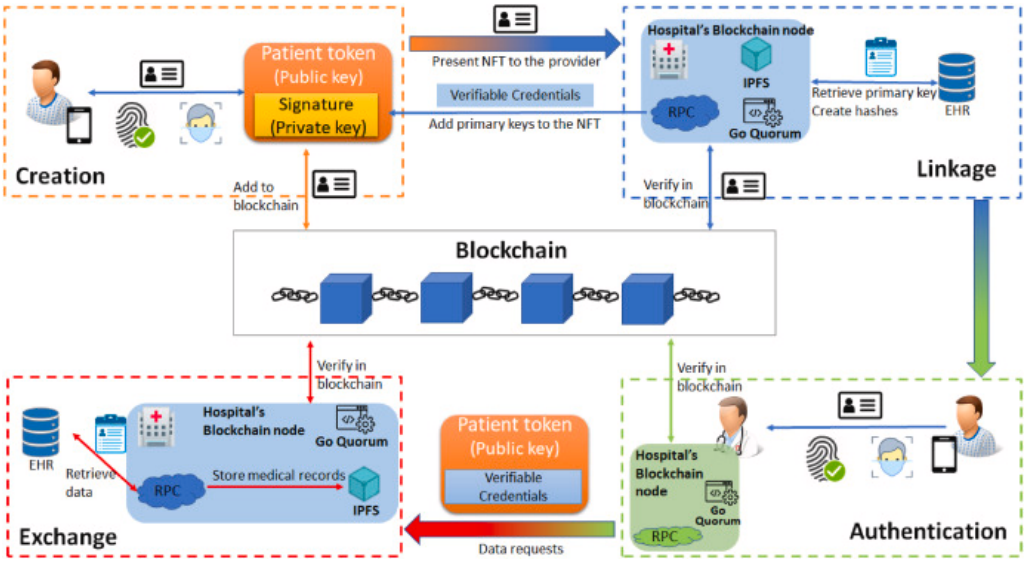

Figure 17: Four modules contained in the overall architecture for the use of NFT for HIE authentication, beginning with the creation of NFTs through blockchain, followed by the linkage of remote patient IDs across healthcare facilities, and ending with patient authentication for ownership of NFTs and permission for healthcare providers to retrieve their medical history in the final Exchange module.

The proposed solution represents an improvement by introducing patient-centric control over the sharing of medical records. Patients are empowered to create NFTs on their mobile devices, linking their biometric information securely. The linkage module establishes connections across healthcare facilities, unifying patient identification through a master patient index table on the blockchain. The authentication module employs Self-Sovereign Identity (SSI) principles, allowing patients to validate their identity using biometrics stored locally on their devices. The exchange module facilitates secure and authorized data exchange between patients and healthcare providers.

The author's evaluation of the solution involves a detailed description of the back-end activities of each module, including the creation of NFTs, linkage of patient IDs, authentication, and the HIE process. The use of the Diffie–Hellman key exchange protocol and the Quorum blockchain is presented as the underlying technology supporting the security and privacy aspects of the solution.

What is your analysis of the identified problem, idea and evaluation? Is this a good idea? What flaws do you perceive in the work? What are the most interesting or controversial ideas? For work that has practical implications, ask whether this will work, who would want it, what it will take to give it to them, and when might it become a reality?

In terms of analysis, the proposed solution appears to be a promising idea, addressing the challenges of patient matching, data security, and interoperability in HIE. The use of NFTs for patient identification and the patient-centric control over data sharing are interesting and potentially transformative concepts.

Possible flaws in the work could include concerns related to the security of bio-

metric information stored on patients' mobile devices and the reliance on blockchain technology, which may face scalability challenges in real-world implementations. Additionally, the practical implications of deploying such a system in a large-scale healthcare environment need to be carefully considered, including issues of user adoption, regulatory compliance, and interoperability with existing healthcare systems.

What are the paper's contributions (author's and your opinion)? Ideas, methods, software, experimental results, experimental techniques...?
The contributions of the paper lie in introducing a comprehensive solution to HIE authentication using blockchain and NFTs, detailing the technical aspects of each module, and emphasizing patient-centric control and privacy. The use of the Quorum blockchain and the Diffie–Hellman key exchange protocol adds to the robustness of the proposed solution.
What are future directions for this research (author's and yours, perhaps driven by shortcomings or other critiques)?
The authors have outlined several future directions for their research. They plan to:

Continue assessing the blockchain protocol and formulate strategies to address its scalability issue. Explore the potential of Non-Fungible Tokens (NFTs) in important data exchanges, such as integrating NFTs with the cryptocurrency concept to establish an incentive mechanism for data sharing. Provide a comprehensive functionality design for Health Information Exchange (HIE), such as personalized data segmentation, partial Electronic Health Record (EHR) indexing, and smart contracts for regulation enforcement, based on NFT authentication. Conduct large-scale simulations using real-world data to further evaluate the feasibility, stability, scalability, and security of the system. In addition to these, some potential directions could include:

Investigating the interoperability of the proposed system with existing healthcare IT infrastructure. Evaluating the economic implications of implementing such a system, including the cost of NFT transactions.
What questions are you left with? What questions would you like to raise in an open discussion of the work (review interesting and controversial points, above)? What do you find difficult to understand? List as many as you can.

1. How will the proposed incentive mechanism for data sharing work in practice?
2. What measures will be taken to ensure the accuracy and integrity of the data being exchanged?
3. How will the system handle potential disputes or disagreements over data ownership or authenticity?

4. How will the proposed system interact with existing laws and regulations related to healthcare data exchange?
5. What are the potential risks or downsides of using NFTs in this context, and how might they be mitigated?
6. What are the specific use cases for the application of NFTs in healthcare data exchange? Can some examples be provided?
7. What are the technical requirements for healthcare providers to participate in this system? Will special training be needed?

A.6: Blockchain-Enabled Secure and Smart Healthcare System [49]

Authors: Das, Debendranath and Muthaiah, Amudhan and Ruj, Sushmita.

Published in: May 2022

What is your take-away message from this paper?
The take-away message from this paper is that blockchain technology can be effectively utilized to create a secure and fair healthcare system. The proposed system ensures transparency, privacy, and fairness for both patients and hospitals. By integrating blockchain and smart contracts, the system provides a mechanism for secure exchange of medical data, fair financial transactions, and accountability for all parties involved. The paper also presents the implementation and evaluation of the prototype on the Ethereum platform, demonstrating the feasibility and potential of blockchain-enabled healthcare systems.

What is the motivation for this work (both people problem and technical problem), and its distillation into a research question? Why doesn't the people problem have a trivial solution? What are the previous solutions and why are they inadequate?
The motivation for this work stems from the existing problems in the healthcare sector, both from a people problem and a technical problem perspective. The people problem involves the lack of transparency and trust issues between patients and hospitals, leading to overcharging, inadequate treatment, and potential mistreatment. The technical problem is related to the security and privacy of patients' medical data, which is at risk of unauthorized access, tampering, and misuse. The distillation into a research question can be summarized as follows: "How can blockchain technology be leveraged to create a secure and fair healthcare system that addresses the lack of transparency, trust issues, and privacy concerns, while ensuring fairness for both patients and hospitals?" The people problem does not have a trivial solution because it involves complex issues of trust, fairness, and privacy in the healthcare system, which cannot be easily addressed using traditional centralized approaches. Previous solutions have attempted to use blockchain and other technologies to address healthcare data security and transparency issues. However, these solutions have been inadequate due to various drawbacks such as single points of failure, lack of scalability, key management problems, and the inability to guarantee fairness for all entities involved. The paper highlights these inadequacies and presents a novel approach to address these challenges.

What is the proposed solution (hypothesis, idea, design)? Why is it believed it will work? How does it represent an improvement? How is the solution achieved? What is the author's evaluation of the solution? What logic, argument, evidence, artifacts (e.g., a proof-of-concept system), or experiments are presented in support of the idea?

The proposed solution in the paper is a blockchain-enabled Secure and Smart Healthcare System. The hypothesis is that by integrating blockchain technology with smart contracts, it is possible to create a system that ensures transparency, privacy, and fairness in healthcare transactions. The idea is to use blockchain to provide a secure and immutable ledger for storing patients' medical data, while smart contracts are used to enforce fair interactions between patients and hospitals.

The authors believe that this solution will work because blockchain technology provides a decentralized, tamper-proof, and transparent platform for storing and exchanging sensitive medical data. Smart contracts enable the automation of processes and ensure that all parties involved adhere to predefined rules and agreements. This solution represents an improvement over previous approaches by addressing the lack of transparency, trust issues, and privacy concerns in the healthcare system, while also ensuring fairness for both patients and hospitals.

The solution is achieved by implementing three smart contracts: one for the interaction between patients and hospitals, one for the interaction between patients and the medical database owner, and one for registration of entities in the system. These smart contracts define the rules and processes for accessing medical data, financial transactions, and dispute resolution.

The authors evaluate the solution by implementing a prototype on the Ethereum platform and Ropsten test network. They provide an analysis of the performance of the system, including the cost of deployment, transaction costs, and time taken for various functions. The paper also presents the logic and algorithms used in the smart contracts, as well as the implementation details of the Fairswap Protocol for fair exchange of information between patients and the database owner. The evidence presented includes the successful deployment of the smart contracts and the performance metrics obtained during the evaluation.

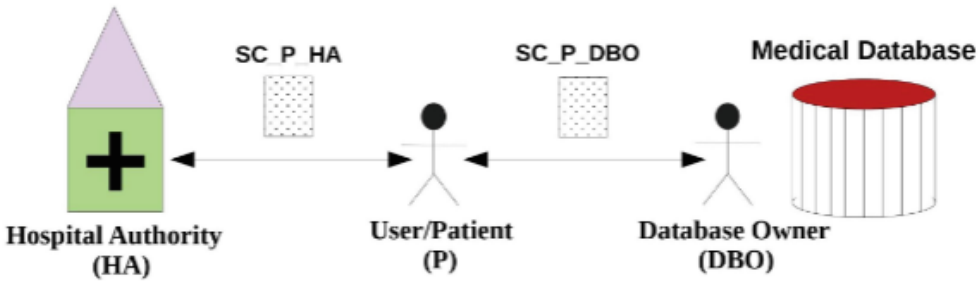

Figure 18: simple overview of the system

What is your analysis of the identified problem, idea and evaluation? Is this a good idea? What flaws do you perceive in the work? What are the most interesting or controversial ideas? For work that has practical implications, ask whether this will work, who would want it, what it will take to give it to them, and when might it become a reality?

The identified problem of lack of transparency, trust issues, and privacy concerns

in the healthcare system is a significant issue that has practical implications for patients, hospitals, and other entities involved in healthcare transactions. The idea of using blockchain and smart contracts to address these problems is promising, as it leverages the inherent security, transparency, and automation capabilities of blockchain technology. The evaluation of the solution through the implementation of a prototype and analysis of performance metrics provides valuable insights into the feasibility and potential of the proposed system.

However, there are some flaws and challenges that can be perceived in the work. One potential flaw is the assumption of the database owner being semi-trusted, which may not hold true in all real-world scenarios. Additionally, the practical implementation of the proposed system on a large scale, including integration with existing healthcare infrastructure and compliance with regulatory requirements, may present challenges.

The most interesting and controversial ideas in the work revolve around the use of blockchain to address trust and privacy issues in healthcare. The concept of fair exchange of information between patients and healthcare providers using smart contracts is also intriguing, as it introduces a new paradigm for ensuring fairness in healthcare transactions.

For work that has practical implications, the question of whether this idea will work depends on various factors such as regulatory acceptance, adoption by healthcare providers, and the ability to integrate with existing systems. Stakeholders who would want this solution include patients, healthcare providers, and regulatory authorities who are concerned about data security and fairness in healthcare transactions. Giving it to them would require addressing the practical challenges of implementation, ensuring compliance with healthcare regulations, and providing user-friendly interfaces for all parties involved.

The reality of widespread adoption of blockchain-enabled healthcare systems may take time, as it involves significant changes to existing processes and infrastructure. However, with increasing awareness of data security and privacy concerns in healthcare, coupled with advancements in blockchain technology, the potential for this solution to become a reality in the near future is promising.

What are the paper's contributions (author's and your opinion)? Ideas, methods, software, experimental results, experimental techniques...?

The paper's contributions are significant and encompass several key aspects:

1.Novel Idea: The paper introduces a novel concept of a blockchain-enabled Secure and Smart Healthcare System, addressing the lack of transparency, trust issues, and privacy concerns in the healthcare sector. The integration of blockchain and smart contracts to ensure fairness, privacy, and security in healthcare transactions is a valuable and innovative idea.

2.Methodology: The paper presents a detailed methodology for implementing the proposed system, including the use of smart contracts, cryptographic primitives,

and the Fairswap Protocol for fair exchange of information. The methodology provides a clear and structured approach to addressing the identified problems in the healthcare system.

3.Software Implementation: The authors have implemented a prototype of the proposed system on the Ethereum platform and Ropsten test network. This practical implementation demonstrates the feasibility of the proposed solution and provides valuable insights into the performance and cost considerations.

4.Experimental Results: The paper presents an analysis of the performance of the system, including deployment costs, transaction costs, and time taken for various functions. The experimental results provide evidence of the practical viability of the proposed system.

5.Evaluation Techniques: The paper employs rigorous evaluation techniques to assess the performance and feasibility of the proposed solution. The use of real-world implementation and analysis of performance metrics adds credibility to the findings.

In my opinion, the paper's contributions are significant in advancing the understanding of how blockchain technology and smart contracts can be leveraged to address critical issues in the healthcare sector. The practical implementation and evaluation of the proposed system provide valuable insights for researchers, practitioners, and policymakers in the healthcare and technology domains. The methodology and experimental results presented in the paper contribute to the body of knowledge in the field of blockchain-enabled healthcare systems.

What are future directions for this research (author's and yours, perhaps driven by shortcomings or other critiques)?

Future directions for this research could encompass several areas, driven by the identified shortcomings and potential critiques:

1.Enhanced Privacy Measures: One potential future direction could involve further enhancing the privacy measures within the proposed system. This could include exploring advanced encryption techniques, zero-knowledge proofs, or privacy-preserving algorithms to ensure the highest level of data security and privacy for patients' medical records.

2.Regulatory Compliance: Addressing the regulatory compliance aspect is crucial for the practical implementation of the proposed system. Future research could focus on understanding and addressing the legal and regulatory requirements related to healthcare data management and financial transactions, ensuring that the proposed system aligns with existing healthcare regulations.

3.Scalability and Interoperability: As blockchain technology continues to evolve, future research could focus on addressing scalability and interoperability challenges. This could involve exploring solutions to handle a large volume of healthcare transactions and ensuring seamless integration with existing healthcare information systems.

4.Real-world Implementation Studies: Conducting real-world implementation studies and pilot projects to deploy the proposed system within healthcare organizations would be a valuable future direction. This would provide insights into the practical challenges, user acceptance, and the impact of the system on healthcare operations.

5.User Experience and Adoption: Future research could focus on understanding the user experience and adoption of blockchain-enabled healthcare systems. This could involve user studies, feedback collection, and iterative improvements to ensure that the system is user-friendly and meets the needs of all stakeholders, including patients, healthcare providers, and regulatory authorities.

6.Economic and Cost Considerations: Exploring the economic and cost implications of implementing blockchain-enabled healthcare systems would be valuable. This could involve conducting cost-benefit analyses, assessing the long-term financial implications, and understanding the return on investment for healthcare organizations.

7.Security and Resilience: Further research could focus on enhancing the security and resilience of the proposed system against potential cyber threats, data breaches, and adversarial attacks. This could involve exploring advanced security mechanisms and threat modeling specific to healthcare environments.

These future directions, driven by the identified shortcomings and critiques, would contribute to the continued advancement and practical implementation of blockchain-enabled secure and smart healthcare systems.

What questions are you left with? What questions would you like to raise in an open discussion of the work (review interesting and controversial points, above)? What do you find difficult to understand? List as many as you can.

1. **Scalability:** How does the proposed system address scalability concerns, especially when dealing with a large volume of healthcare transactions and data?
2. **Interoperability:** How does the proposed system ensure interoperability with existing healthcare information systems and standards? Are there any potential challenges in integrating with legacy systems?
3. **Regulatory Compliance:** What are the specific regulatory and legal considerations that need to be addressed for the practical implementation of the proposed system in different healthcare jurisdictions?
4. **User Acceptance:** What are the potential barriers to user acceptance of blockchain-enabled healthcare systems, and how can these be mitigated? What are the user experience implications for patients, healthcare providers, and other stakeholders?

5. **Cost Implications:** What are the long-term cost implications for healthcare organizations in implementing and maintaining a blockchain-enabled healthcare system? How does the potential return on investment compare to traditional healthcare systems?

6. **Data Privacy:** How does the proposed system ensure compliance with data privacy regulations such as GDPR and HIPAA? Are there any specific challenges related to data privacy that need to be addressed?

7. **Real-world Implementation:** What are the practical challenges and considerations in implementing the proposed system within healthcare organizations? Are there any case studies or pilot projects that demonstrate the real-world feasibility of the system?

8. **Security and Resilience:** How does the proposed system address potential security threats and adversarial attacks? What are the mechanisms in place to ensure the resilience of the system against cyber threats?

9. **Ethical Considerations:** What ethical considerations need to be taken into account when implementing blockchain technology in healthcare, especially concerning patient data and consent?

10. **Cost and Performance Trade-offs:** How do the cost and performance trade-offs of the proposed system compare to traditional healthcare systems? Are there any specific areas where the proposed system excels or falls short?

11. **Adoption Challenges:** What are the potential challenges in the widespread adoption of blockchain-enabled healthcare systems, and how can these be addressed?

12. **Long-term Viability:** What are the long-term implications and viability of blockchain technology in the healthcare sector, considering the rapidly evolving nature of both technology and healthcare regulations?

10 Appendix B : Sequence Diagrams for Rosheta

10.1 Patient login and features

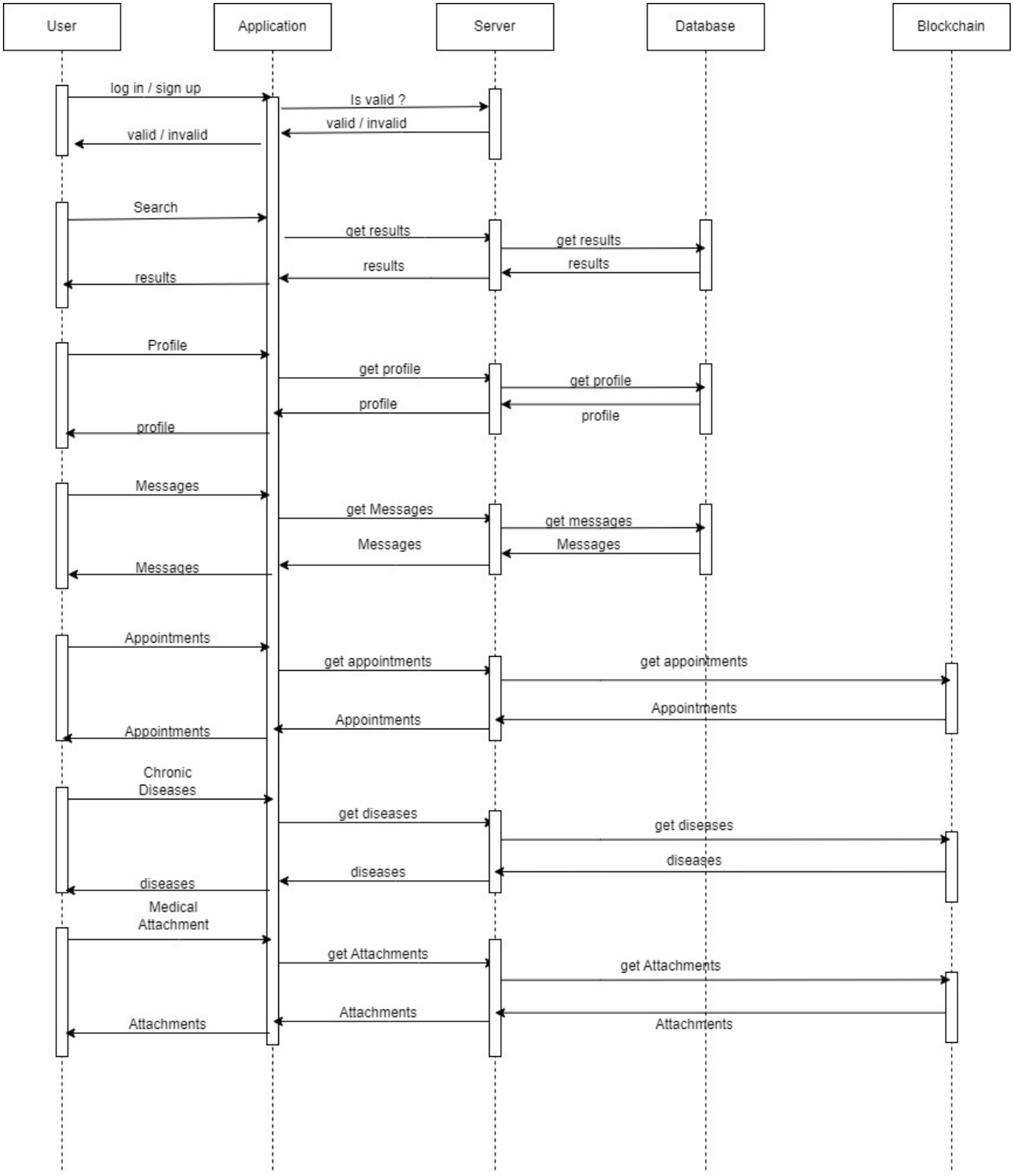

Figure 19: Sequence diagram for patient login and features

10.2 Doctor login and features

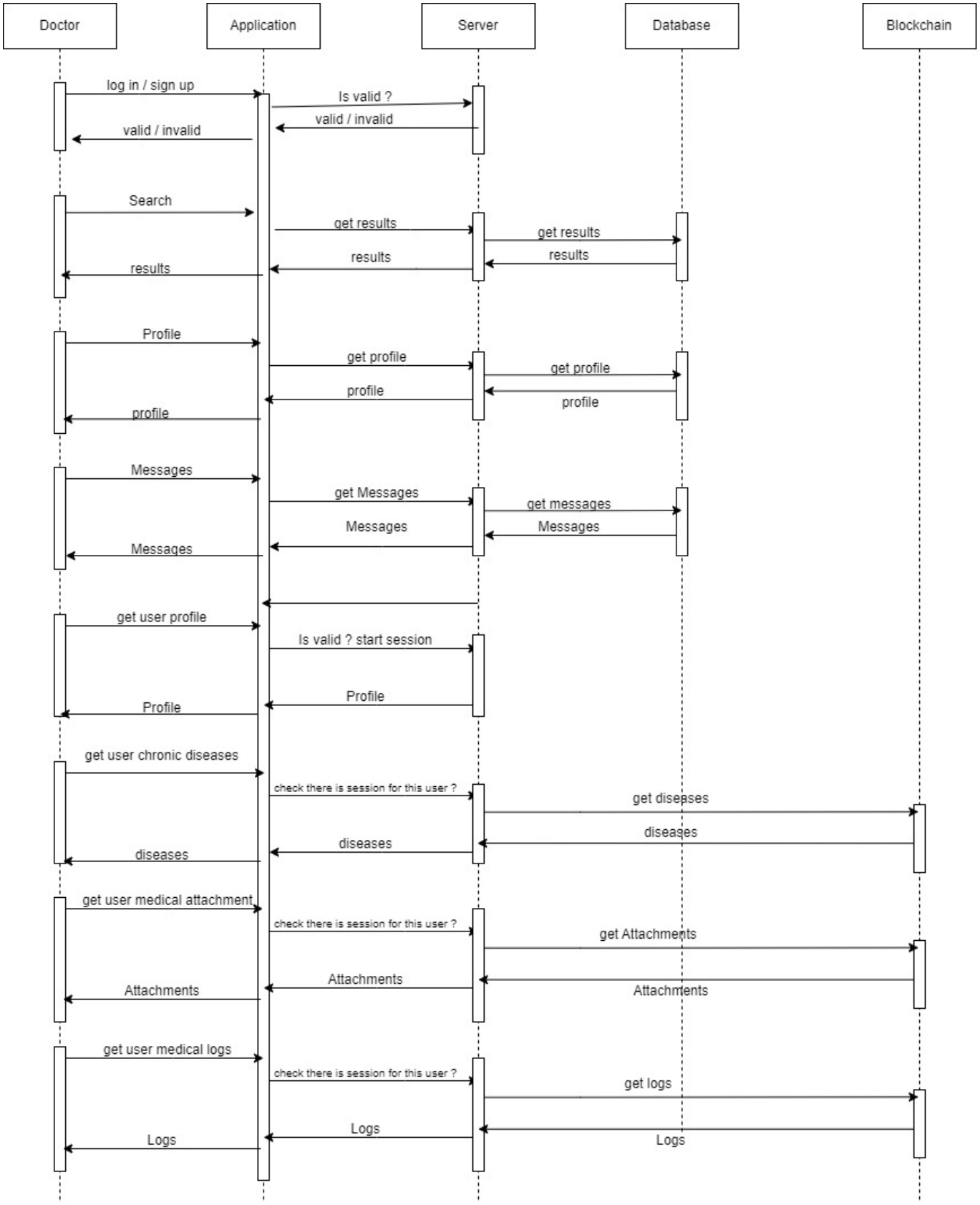

Figure 20: Sequence diagram for doctor login and features

10.3 Search

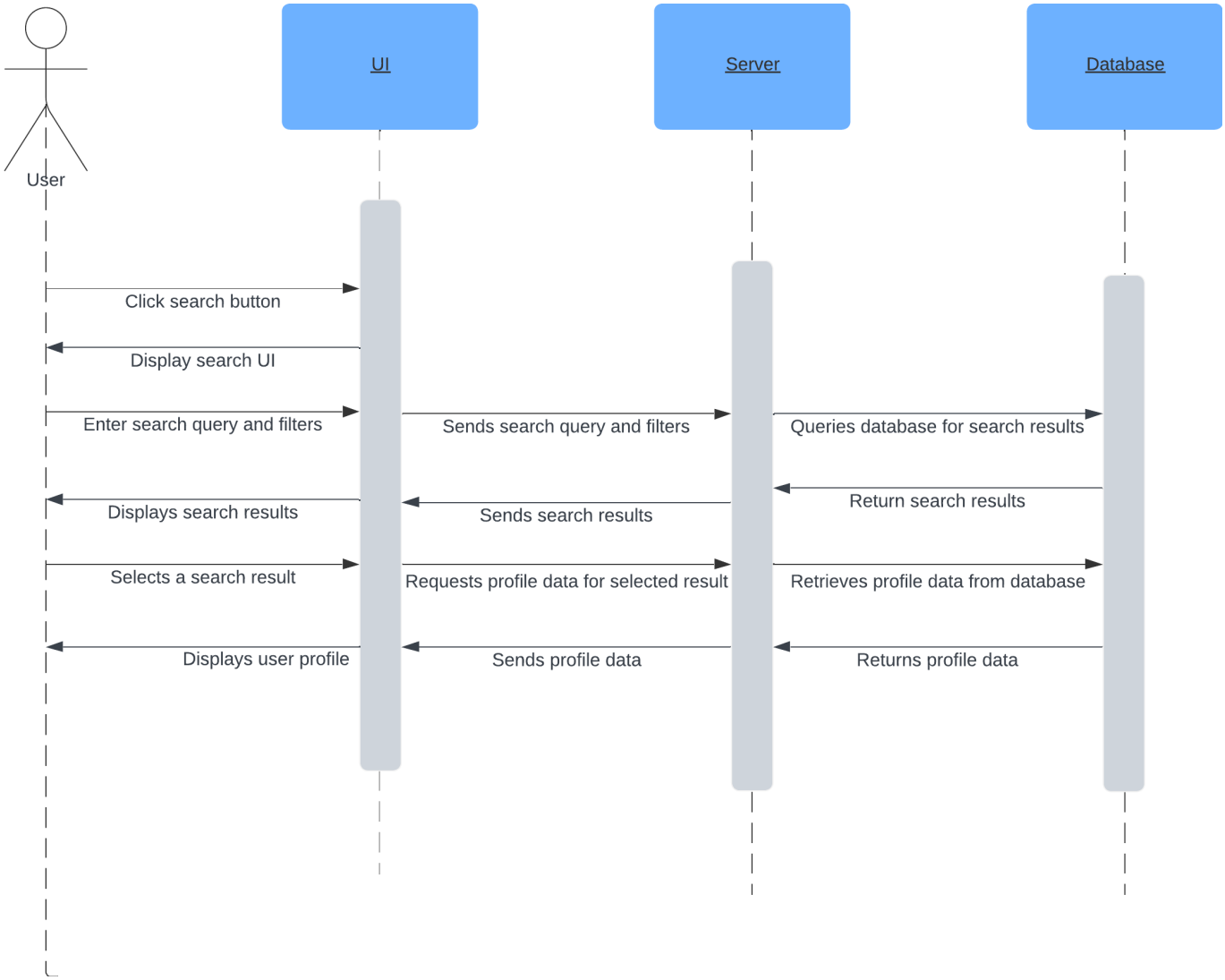

Figure 21: Sequence diagram for search

10.4 See attachment files

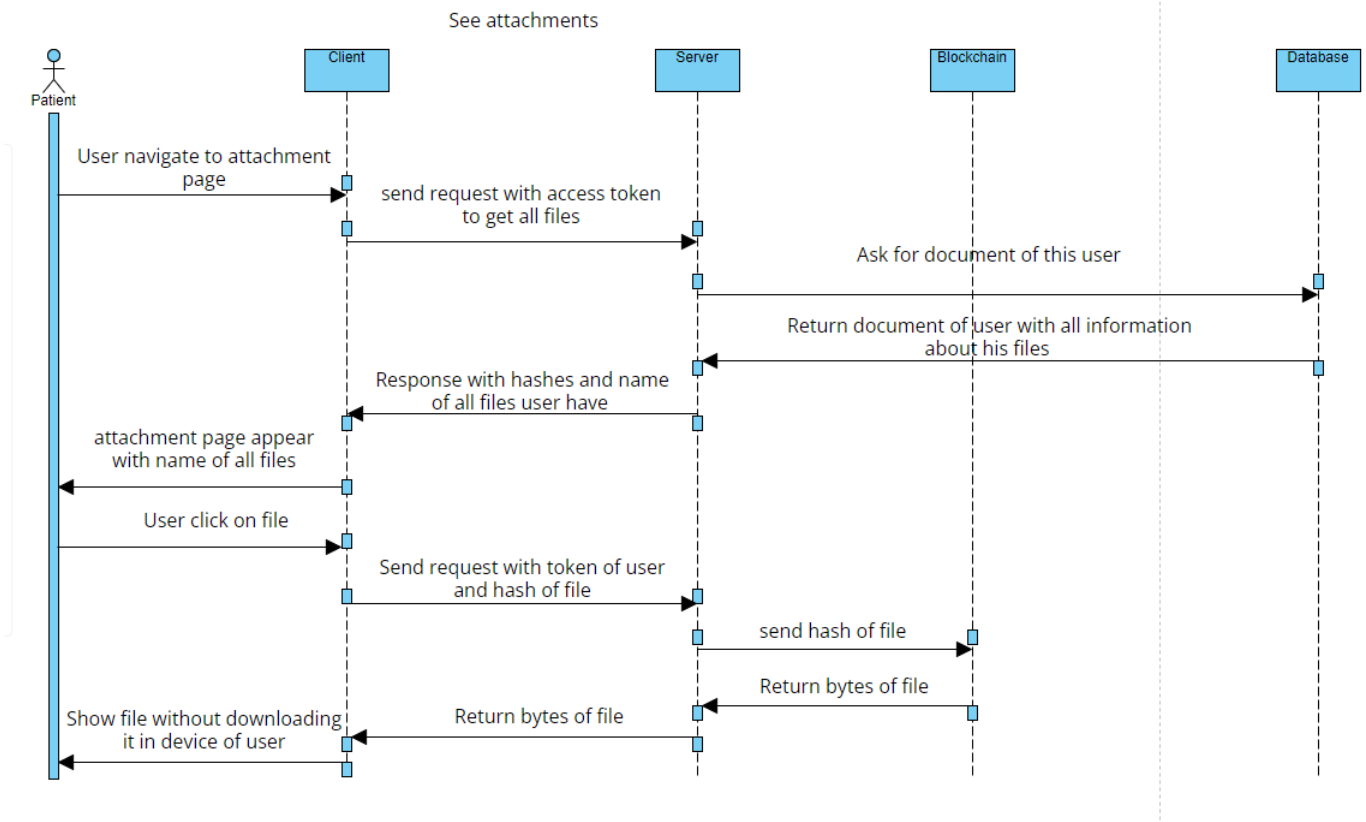

Figure 22: Sequence diagram showing how the patient can see his/her attachment files

10.5 Upload attachment

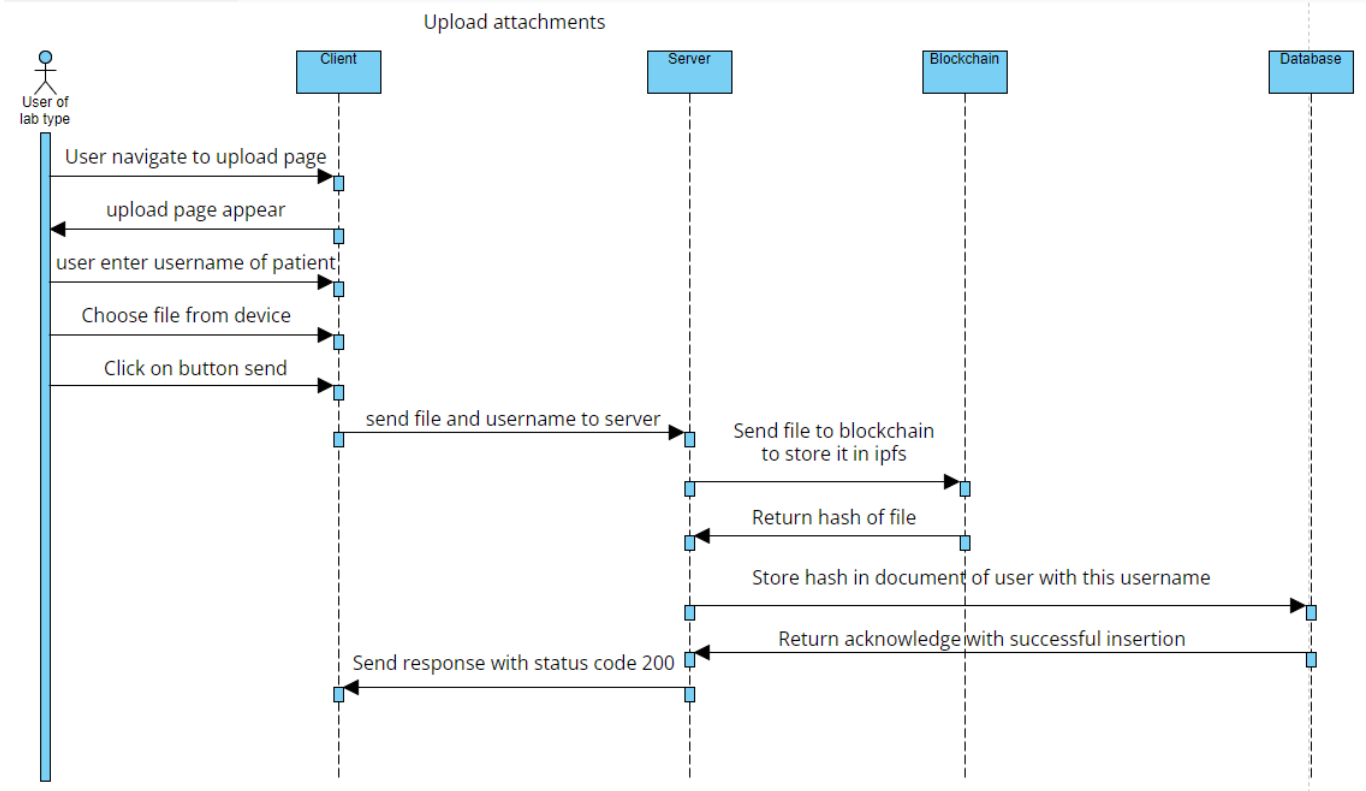

Figure 23: Sequence diagram for uploading the attachments files

10.6 see diseases

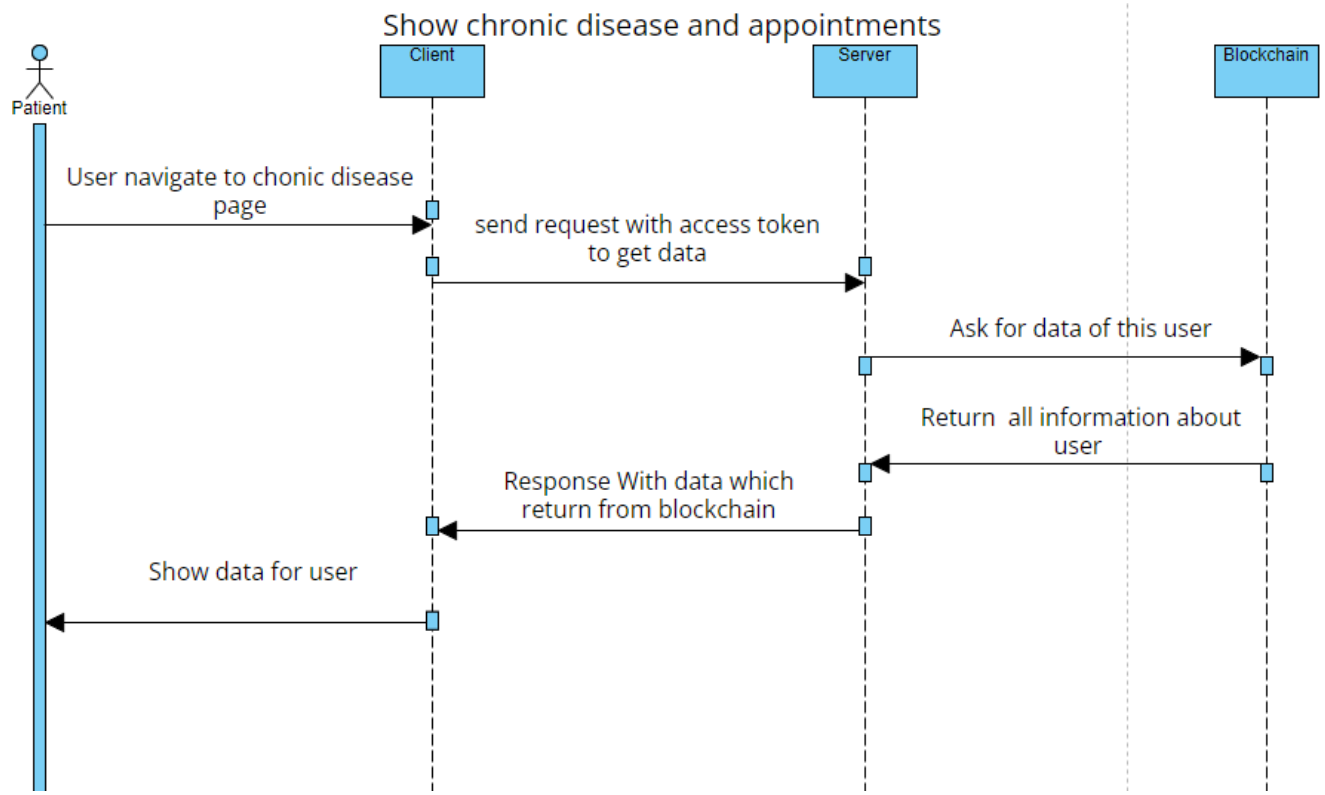

Figure 24: Sequence diagram showing how the patient can see his/her diseases

11 Appendix C : UI samples of Rosheta

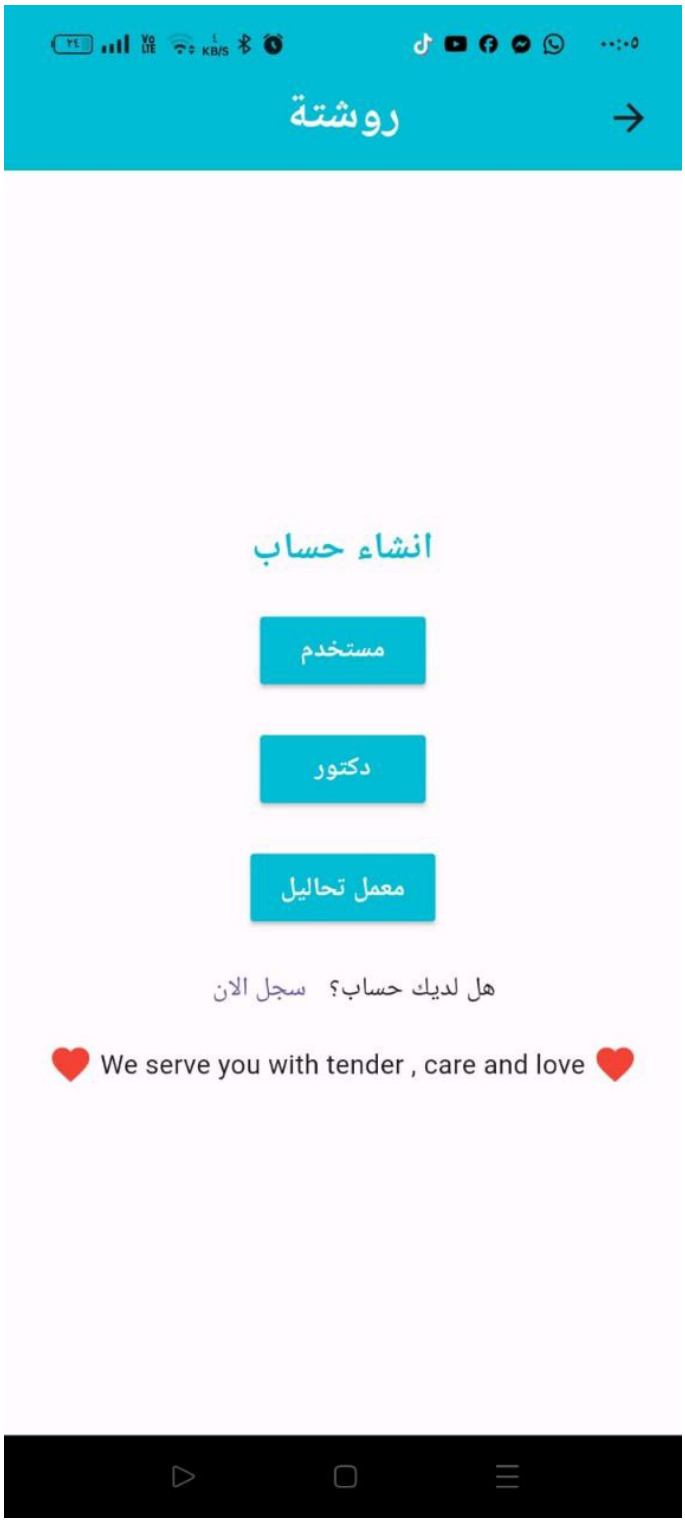

Figure 25: Choose the account type to register

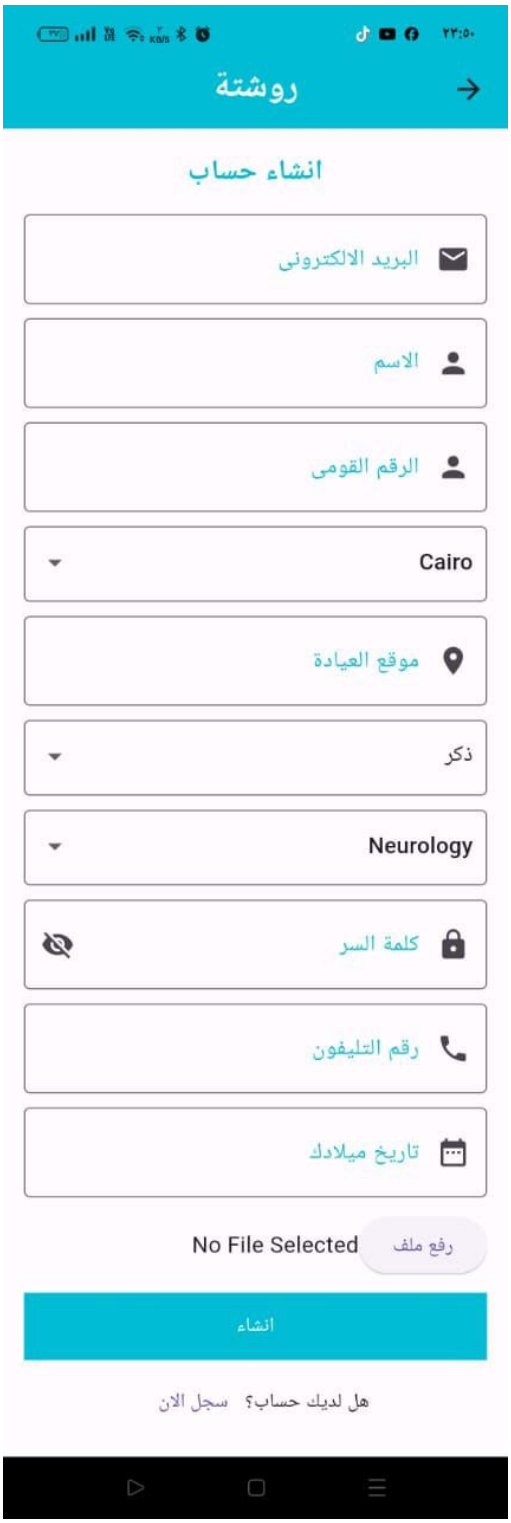

Figure 26: Register as doctor

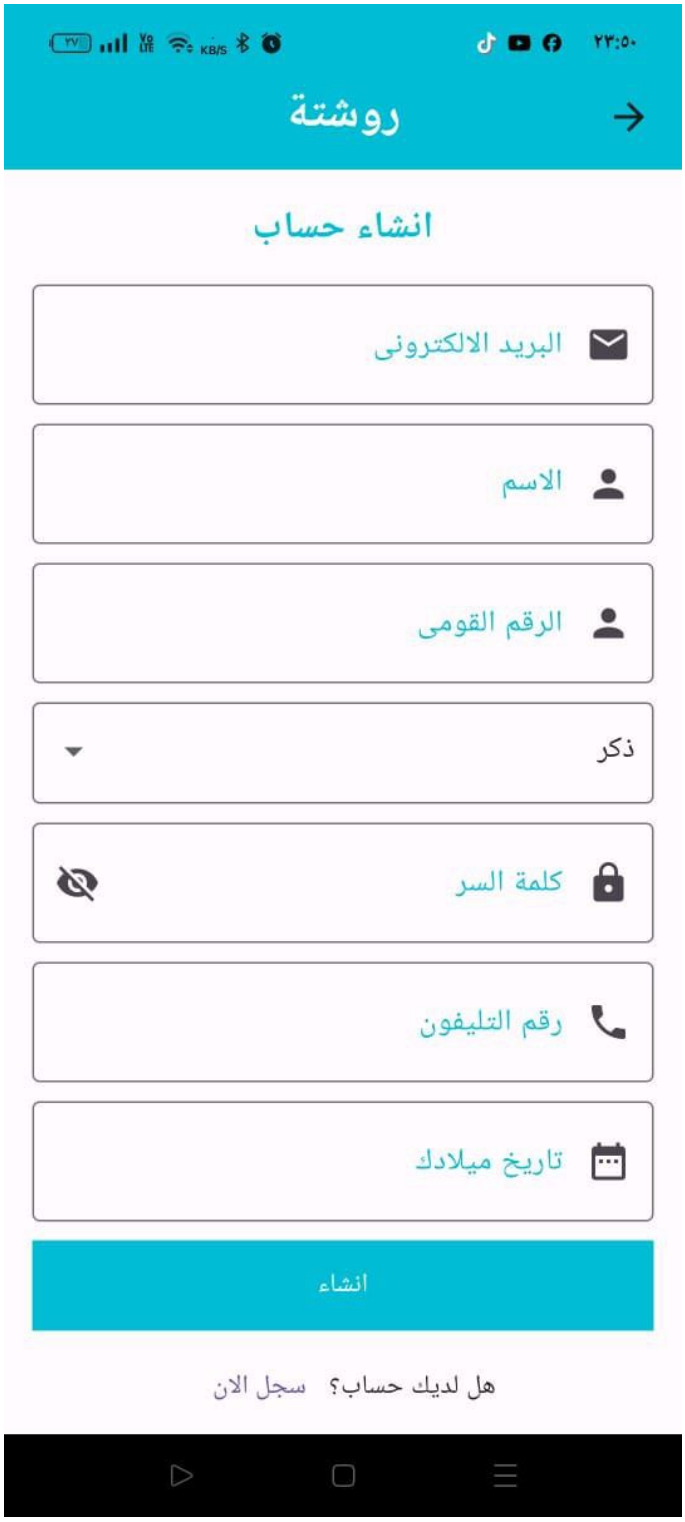

Figure 27: Register as patient

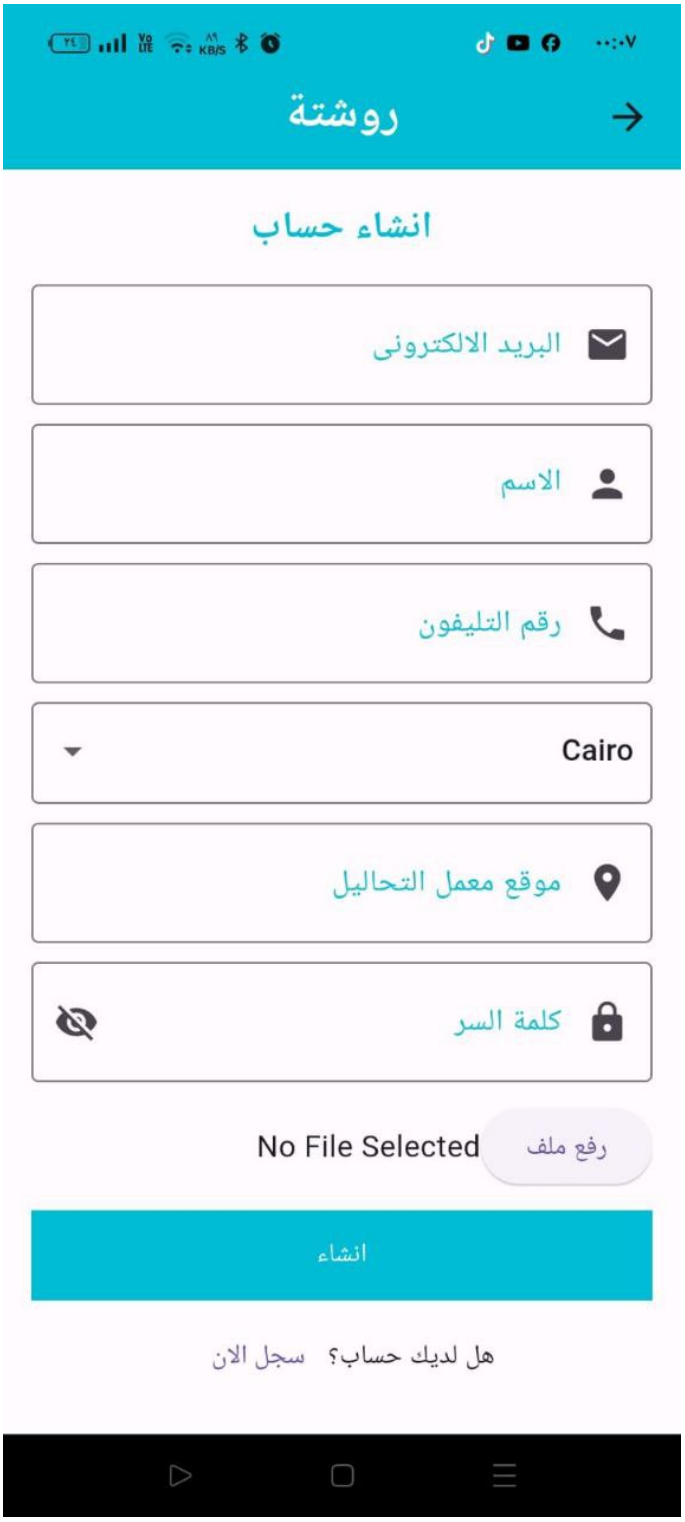

Figure 28: Register as lab

Figure 29: Doctor profile sample

Figure 30: modify your profile sample

Figure 31: messages in chat

Figure 32: chats page

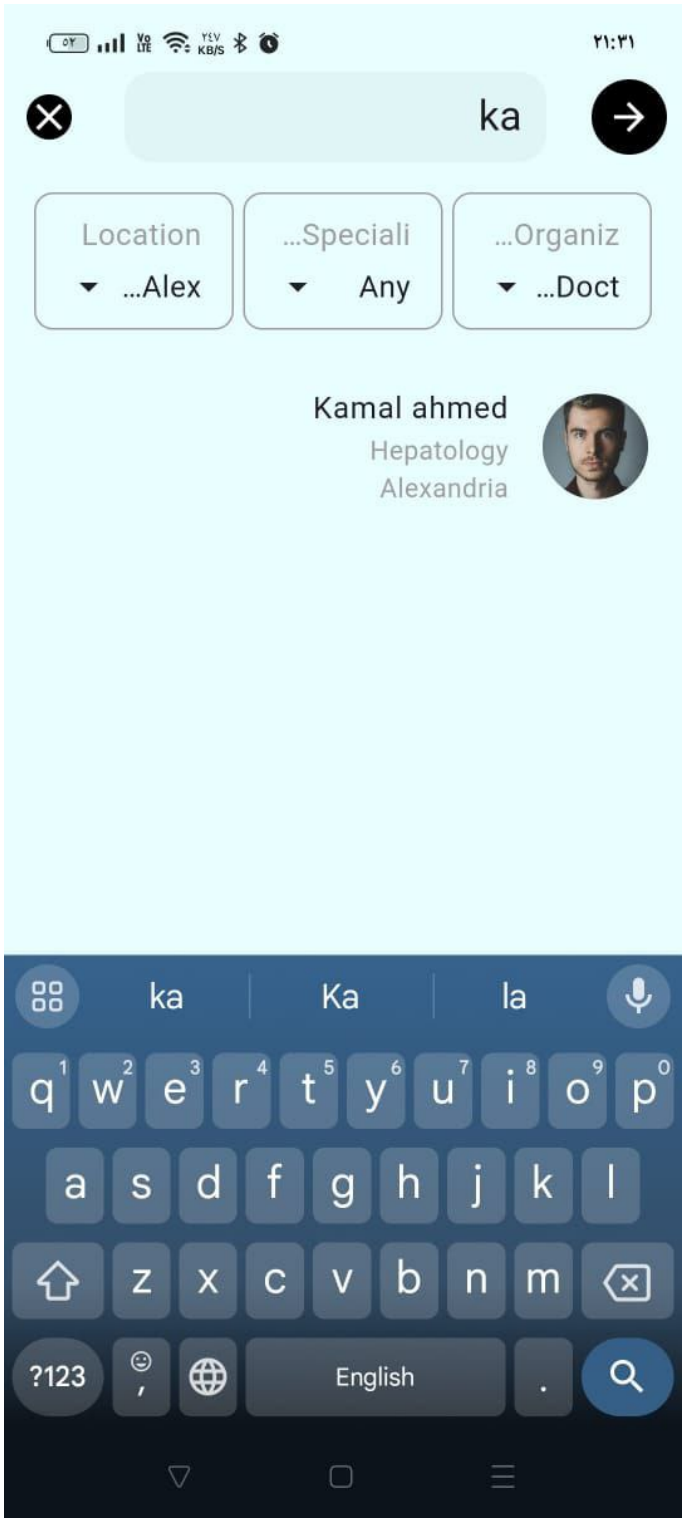

Figure 33: search for doctor

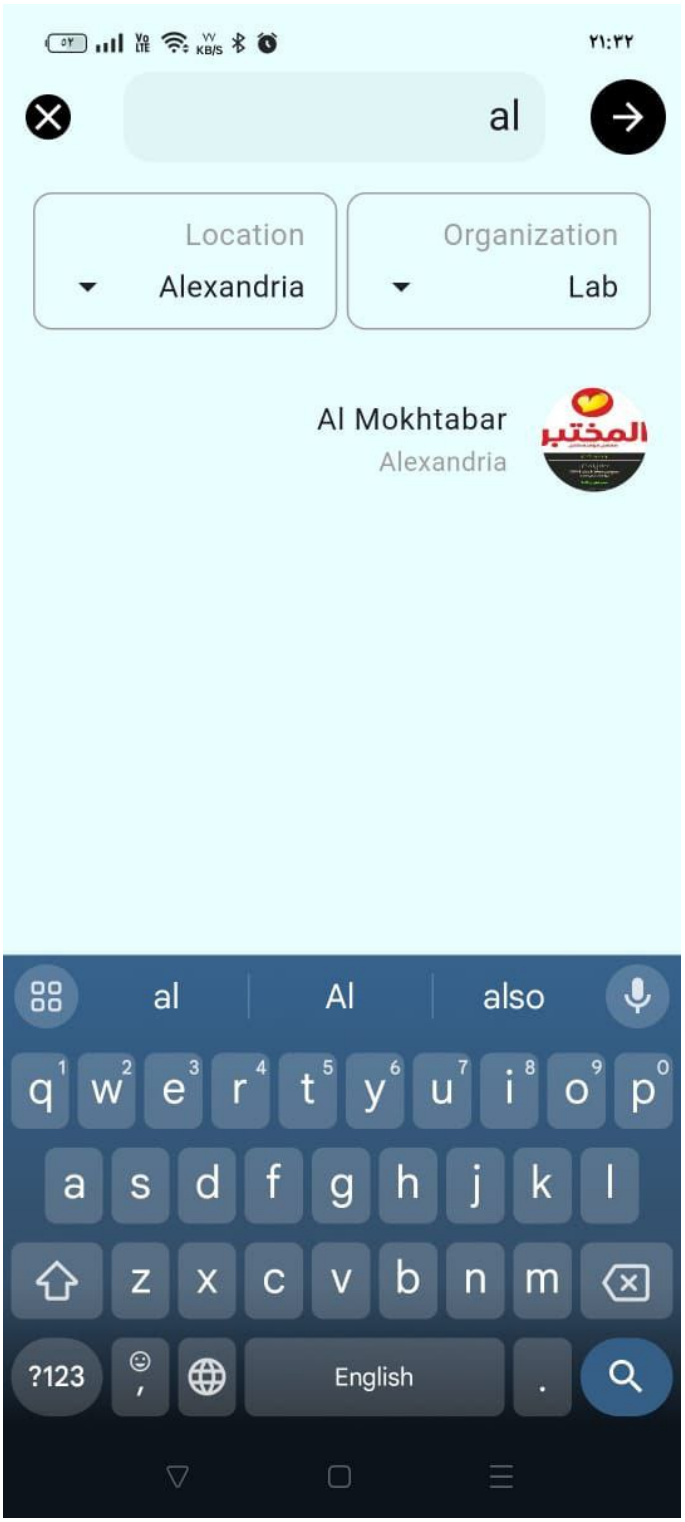

Figure 34: search for lab

Figure 35: Search Screens

Figure 36: request access from patient

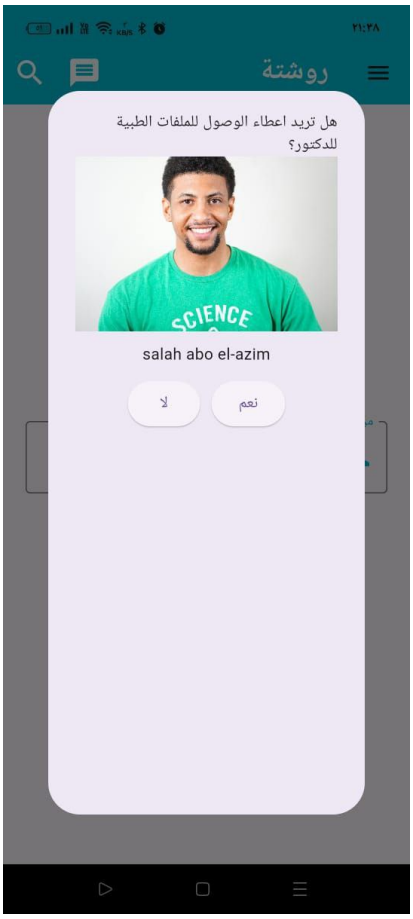

Figure 37: patient confirmation message

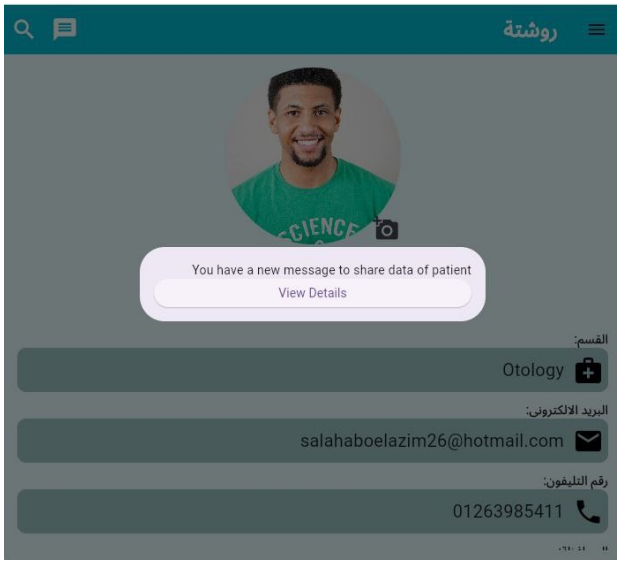

Figure 38: doctor got a notification

Figure 39: doctor can access all medical history

Figure 40: Registration Screens

Figure 41: doctor can add new record

Figure 42: doctor can see the chronic diseases

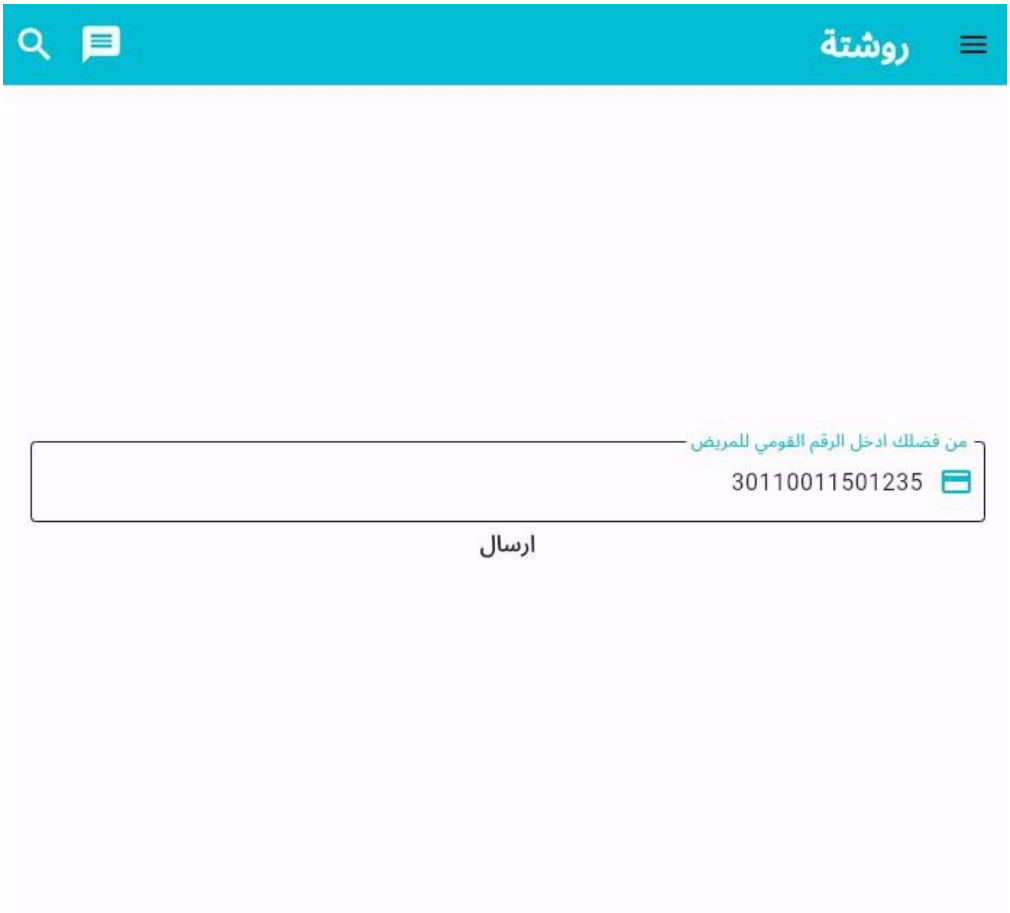

Figure 43: enter patient national Id to access their data

Figure 44: message to patient in emergency cases