Decentralised Telehealth Data through Blockchain Technology: A ledger between physical and online health services.

Research Project

Programme Name: MSc. Cybersecurity

Tochukwu Christopher Nwosu

Student ID: x20257457

School of Computing

National College of Ireland

Supervisor: Dr. Vanessa Ayala-Rivera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: …. Tochukwu Christopher Nwosu………………………………………………………………….

Student ID: …… x20257457 …………………………………………………………………...………….

Programme:……MSc Cybersecurity…………… **Year:** …2022……………………

Module: ……Research Project…………………………………………………………………….……………

Supervisor: …… Dr. Vanessa Ayala-Rivera…………………………………………………………….…………

Submission Due Date: ……25/04/2023……………………………………………………………………….……………

Project Title: Decentralised Telehealth Data through Blockchain Technology: A ledger between physical and online health services………………………………………………………………………….…………

Word Count: ……6,700…………………………… **Page Count**………………20………………………….......

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……***T.C.N***……………………………………………………………………………………...

Date: ……25/04/2023………………………………………………………………………………….

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Decentralised Telehealth Data through Blockchain Technology: A ledger between physical and online health services.

Tochukwu Christopher Nwosu

Student ID: x20257457

Abstract

Blockchain is a critical innovation that can improve delivery of services in the healthcare sector. This project examined a decentralized health system using blockchain technology. The project particularly focused on establishing a decentralized system using distributed ledger between physical and online health services. The project was aimed at using blockchain technology to update healthcare data in the online database. In addition, the project was aimed at demonstrating that blockchain technology could be used to improve the integrity and privacy of data in the health sector. The project highlighted that the decentralized blockchain system is applied in other sectors such as finance, retail and real estate. Therefore, similar approaches and techniques could be employed to create a decentralized healthcare system that could guarantee data integrity. The development of the project involved a review of other blockchain technologies such as Medical Chain, MedCredits and MyHealthMyData. Besides, the project employed a flowchart that highlighted the different phases covered in the development of a decentralized telehealth system. The implementation of the system used tools and components such as Flutter, Solidity and Truffle. Ethereum blockchain was used in the project to develop a smart contract and retrieve data. The project constituted two experiments including testing how blockchain technology could help to update healthcare data and enhance data integrity and privacy. Updating data in online databases involved steps such as creation, verification and broadcasting of transactions, mining, adding the block to the chain and updating the ledger. Enhancing data integrity, on the other hand, involved setting up access permissions, creating anonymous transactions and establishing a consensus algorithm. The development of an application for a decentralized healthcare system demonstrated that blockchain is critical in enhancing service delivery through updating data in online databases as well as ensuring data integrity in the health sector. However, there is a need for further research on aspects such as developing advanced and secure telehealth systems that are tailored to specific medical conditions, integration of virtual and augmented reality and creating a telehealth platform that enables real-time communication among healthcare providers.

1 Introduction

The emergence of the COVID-19 pandemic defined a key moment of adjustments in service delivery in the health sector. Patients and doctors were required to maintain social distance to minimise infections. This necessitated the implementation of resilient and robust systems to protect all parties in the health sector from infections. For instance, telemedicine facilitated service delivery during the pandemic since it prevented physical meetings of patients and healthcare providers (Temesgen *et al.* 2020). Therefore, there was an increase in utilisation of services from organisation such as JD Health, Teladoc Health and RUMC which provide platforms for telemedicine.

Centralisation threatens service delivery in telemedicine because of the associated risks. According to Mohammed *et al* (2021), one of the critical threats in is the risk of losing data to cyberattacks. Both internal and external breaches can compromise the integrity and reliability of telemedicine systems. In another study, Ahmad *et al.* (2021) stated that breaches can be as a result of malware attacks and cybercriminals. Therefore, the current study employs blockchain technology to address the challenges associated with a centralised health system. A study by Ahmad et al. (2021) emphasized that blockchain technology represents a distributed architecture that manages a common ledger. Technology can therefore help address the challenges associated with tracking patient routes, monitoring medications, and verifying physician credentials.

Research on decentralised health system is necessary to enable the hospital and health experts to distribute the health resources. Therefore, this project facilitates enhancement of patient experience such as through reduced waiting hours. The research also addresses data integrity issues that are prevalent in the centralised health system.

1.1 Objectives of the Study

i. To develop a decentralised health ledger system that serves both physical and online databases.
ii. To determine the use of blockchain in updating healthcare data.
iii. To employ blockchain technology in addressing data integrity in health systems.

1.2 Research Questions

i. What is the role of blockchain technology in updating health data in online databases?
ii. What is the role of blockchain technology in improving data integrity and privacy in shared ledger in healthcare systems?

1.3 Significance of the Project

Medical records need innovation. Patients leave data scattered across various jurisdictions as life events take them away from one provider's data to another. In doing so, they lose easy access to past data, as the provider, not the patient, generally retains primary stewardship. Patients thus interact with records in a broken manner that reflects the nature of how these records are managed. Patients with a huge medical history across many hospitals should not have to keep their history in the form of huge Patients and providers may face significant hurdles in initiating data retrieval and sharing due to economic incentives that encourage "health information blocking".

In the age of online banking and social media, patients are increasingly willing, able and desirous of managing their data on the web and on the go. This work explores a blockchain structure with its backend based on a Rinkeby Test network using Ethereum for its data storage and a smart contract for its data logic. Medical Records are data with sensitive information, and hence using DAPPS with smart contracts ensures safety features essential such as Zero Downtime (i.e. the data associated with a patient is always ready to be fetched and updated), Privacy (A Patient's data should be secured and of limited accessibility to only the people closely associated with the patient), Complete data integrity (The data must not be changed by someone in no authority to do so). This MedRec blockchain implementation seeks to solve this vast fragmentation of patient data by bringing it together and organizing it in the form of a ledger while providing it with the benefits provided by blockchain and DAPPs.

Hence, by implementing medical records on the blockchain we achieve the following features which by other means could only be partially fulfilled or not fulfilled at all.

i. Non-Repudiation of Medical Records, that is, once the prescription is received by a patient from a doctor, the transaction is stored digitally on the blockchain signed by the private keys of both the patient and the doctor, hence if either party refuses to claim the ownership of the transaction, it can be easily detected using the public key of both.
ii. Only the authorized doctor can suggest a prescription that is to be added to the patient records.

iii. The integrity that the prescription once added cannot be modified by any of the parties involved, that is, the doctor, the patient or an attacker trying to harass the patient.

iv. Automated transactions using smart contracts i.e. Once the patient authorizes a doctor to suggest a prescription, money is automatically transferred from the patient's wallet to the patient contract and once the doctor sends a prescription, the money is transferred from the patient contract to the doctor's wallet. The prescription to be sent is based on the mutual trust between the doctor and the patient and is not regulated by the application.

v. The contracts were created with vulnerabilities like Re-entrance, transaction ordering, value underflow-overflow etc. in mind hence the application is safe to use under such circumstances if they shall prevail.

1.4 Structure of the report

The report covers the introduction which provides the background of blockchain in healthcare, motivation for the study, objectives of the study, research questions and the study justification. The report further provides a review of the related work which constitutes previous studies on similar topics. The next section constitutes the methodology which describes the methods, tools and techniques used in the development of the project. Thereafter, the report presents design specification of the project, implementation and evaluation. The report concludes with recommendations for future study on similar subject of decentralised system using blockchain technology.

2 Related Work

2.1 Decentralised Blockchain Ledger System

A decentralised blockchain technology is applicable in different sectors such as finance, real estate and others. The study by Xenya and Quist-Aphetis (2019) demonstrated that blockchain technology was useful in the finance sector since it enabled backing up of financial transactions. The scholars discovered that blockchain technology in the financial sector allows each node to contain copies of financial transactions. This means that coordination on one node does not affect the entire transaction. In a similar study, Bhanushali et al. (2020) explored the use of decentralized blockchain systems and how they can be used to prevent fraud in real estate. According to the study, centralised systems in real estate were vulnerable to risks such as fraud and physical damages to the files. On the contrary, smart contracts in blockchain technology enables possession of the files in digital format. Each block in the system contains a copy of the files and hence eliminating the possibility of fraudulent adjustment or damages as a result of system failure. The studies provide crucial insights to inform the development of decentralised systems in the health sector.

The existing literature demonstrates that blockchain can guarantee the integrity of health data and information. For instance, Sosu, Quist-Aphetsi and Nana (2019) found that cryptographic blockchain could facilitate elimination of cyberattacks which are common with the technological advancements. According to the study, advancement in technology simplifies processes such as accessibility of essential data and information. However, hashing algorithm is critical in verification and validating data that is transmitted through a system. The literature provides key insights that are consistent with the solution developed in this project regarding a shared ledger set up.

2.2 Improving user convenience through a blockchain consensus algorithm

Improvement in service delivery is crucial in enhancing the user convenience and general experience. The study by Mingxiao *et al.* (2017) used the case of consensus algorithm in blockchain to improve efficiency and safety of systems. Consensus algorithm is important in improving system safety and stability through decentralisation. The study also highlighted that consensus algorithms improve the immutability of the system and prevent instances of attacks. Another study by Jain *et al.* (2021) found that distributed blockchain facilitated improvement of user experience in autonomous. Therefore, blockchain technology facilitates improvement of user experience. However, according to the study, the development of decentralised blockchain technology requires further research to address the existing gaps.

Technology development also requires system trust and security. Rui et al. (2020) used the example of the Internet of Things to show the need for a decentralized blockchain system to ensure the security and transparency of online data transmission. According to this research, the development of decentralized blockchain systems will follow certain steps to fill potential gaps. For example, before integrating blockchain consensus mechanisms and smart contract technology, we first analyse the technology (Si et al., 2019). The final step is to implement distributed storage and assess system tamper resistance. Research results highlight the safety, efficacy and feasibility of systems developed through decentralized blockchain technology. However, the scholars focused on decentralized blockchain technology for the Internet of Things, which is not fully applicable to healthcare.

2.3 Blockchain projects in telemedicine

Telemedicine enables effective and efficient service delivery in the healthcare sector. For example, Drago, Gatto, and Ruggeri (2021) write that telemedicine can help healthcare professionals diagnose, treat, and monitor patients without the need to meet in person. Another study by Azaria et al. (2016) reviewed the concept of blockchain technology and its importance in telemedicine. The survey highlighted leading blockchain projects that enhance telemedicine service delivery, including

MedRec, Medileger, Medical Chain, Medlock, Wellinc, Medical Chain and RoboMed. Azaria et al. (2016) described MedRec as an open prototype that uses blockchain smart contracts to create a decentralized healthcare content management system. MedRec's authorization protocol mandates access to medical records when providing data sharing and reviewability. Medical Chain is another leading blockchain-enabled platform applicable to telemedicine. According to Ahmad et al. (2021), Medical Chain will enable physicians to access patient databases and improve service delivery. Additionally, the platform provides patients with regular and direct access to their health information to enhance their wellness process.

Another important telemedicine project is MedCredits. Mannaro and Ibba (2016) found that MedCredits is a secure system that protects users from malicious entities that use reputation-based systems to reward and punish honest and dishonest behavior. I found Additionally, MedCredits has a Token-Curated Registry (TCR) service that allows experts on the network to validate physician credentials, allowing only top-ranked medical professionals to sign up for the platform. Todaro (2020) explores an overview of MedCredits in the healthcare system and finds that the project uses Hippocrates, an easy-to-use software that connects dermatologists and patients. The review showed MedCredits' focus on improving access to healthcare and reducing escalating healthcare costs.

2.4 Challenges in integration of blockchain in healthcare

The use of blockchain technology has helped improve factors such as data integrity and user experience, but further research is needed to fill existing gaps. Durneva, Cousins, and Chen (2020) noted that important improvements have been made in integrating blockchain health information technology into healthcare. However, factors such as security and privacy vulnerabilities are not adequately addressed by blockchain technology. Similarly, Chakraborty, Aich, and Kim (2019) argue that decentralized blockchain systems place high demands on computing power.

3 Research Methodology

3.1 Flowchart for the Study

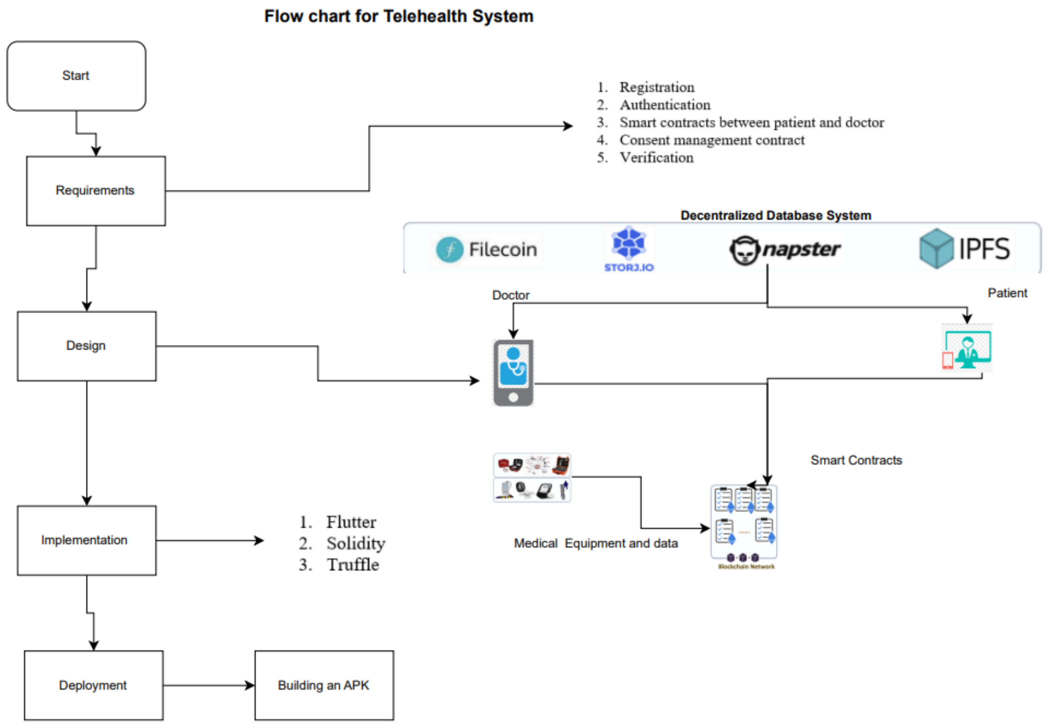

Figure 1: Flowchart of the Telehealth System

Figure 1 illustrates how the telehealth system flows from the initial start to generating an APK.

3.2 Requirements

Figure 1 provides the requirements for the development of the application to enable decentralisation of telehealth system. The requirements include registration, authentication, smart contracts, and verification. In a blockchain telehealth system, patients and doctors will need to register themselves on the platform. The registration process collects basic information about the users such as name, email address and phone number. Additionally, the system requires some form of verification, such as an ID check, to confirm the user's identity. The registration information is securely stored using Ethereum on the blockchain to ensure privacy and data security. After registration, users will need to authenticate themselves to access the platform. This is done using password verification. The authentication mechanism is secured and not easily bypassed to prevent unauthorized access to patient data. In a blockchain telehealth system, smart contracts facilitate transactions between patients and doctors (Hasan *et al.*, 2021). Smart contracts ensure that both parties meet the terms of the contract. Hasan *et al.* (2021) noted that the smart contract could specify the services provided by the doctor and different schedules. In a telehealth system, patients must consent to share their medical data with the doctors. A consent management contract created ensures that patients have explicit consent to share their data.

It is crucial to note that Verification is an essential component of any telehealth system to ensure that patients are receiving medical advice and treatment from licensed and authorized healthcare providers. In a blockchain telehealth system, verification can be done using smart contracts that verify the credentials of healthcare providers before allowing them to participate in the system (Hasan *et al.* 2021). Additionally, the blockchain can also be used to verify patient data, such as medical records, to ensure their accuracy and authenticity.

I, hereinafter as the researcher, considered the key steps of requirement definition, analysis, design, implementation, testing and deployment. The system development focused on both front and backend. The system was also tested to assess the performance capabilities. Shu and Yan (2022) noted that testing of the performance of a system helps to check factors such as robustness in extreme situations. Thereafter, the system is deployed for utility of the users.

4 Design Specification

The implementation of the record-keeping app using Flutter, Solidity, and Truffle relies on a number of techniques, architectures, and frameworks. This section identified and presented some of the key components and their associated requirements as shown in the figure below.

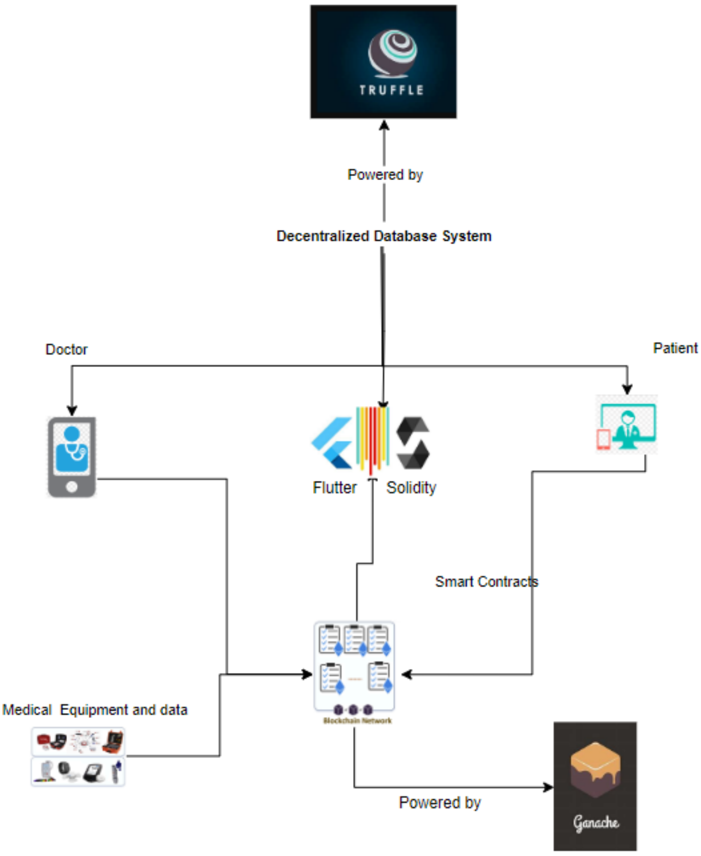

Figure 2: Decentralized database system

Figure 2 provides the components of a decentralized database system including users and the blockchain networks. A decentralized storage network allows the users to store and retrieve data in a distributed manner such as Solidity used in the system (Khan, 2021). In a blockchain telehealth system, Solidity is used to store and manage patients' medical records, ensuring their privacy and security (Shu and Yan, 2022). In a blockchain telehealth system, doctors need to connect to the decentralized system to access patient data securely as shown in the figure above. One way to achieve this is through the use of cryptographic key or smart contract, which is used to authenticate doctors and provide secure access to the data stored on the blockchain. Additionally, doctors can use decentralized applications (dApps) to interact with the blockchain telehealth system, which can provide a secure and user-friendly interface for accessing patient data (Hasan *et al.,* 2021).

The blockchain network is the backbone of a blockchain telehealth system, providing the infrastructure for storing and managing patient data. The blockchain network can be designed to be secure, scalable, and decentralized, ensuring the privacy and security of patient data. To achieve these goals, the blockchain network can use consensus algorithms, such as Proof of Work or Proof of Stake, to ensure the validity of transactions and prevent malicious actors from tampering with the data. Additionally, the blockchain network can use privacy-enhancing technologies, such as zero-knowledge proofs, to ensure the confidentiality of patient data while still allowing doctors to access the necessary information to provide medical treatment (Hasan, *et al.,* 2021).

4.1 Smart Contract Using Truffle and Ethereum

A smart contract is a self-executing contract in which the terms and conditions between the parties are written directly in lines of code (Balcerzak, 2022). The application developed in this project uses smart contracts to store and retrieve data on the Ethereum blockchain. Smart contracts are written in Solidity, a programming language specifically designed for writing smart contracts. Solidity is similar to JavaScript and is used to write code that runs on the Ethereum Virtual Machine (EVM). Truffle is used to deploy smart contracts on the blockchain. Truffle is a development framework for Ethereum that provides a set of tools for creating, testing, and deploying smart contracts. It simplifies the development process by providing a consistent, standardized environment for building blockchain applications (Khan, 2021). Truffle uses the Solidity compiler to compile smart contract code and deploy it to the Ethereum network.

Implementing smart contracts requires knowledge of the Solidity programming language, the Ethereum blockchain, and the Truffle framework. Additionally, they should be familiar with the concepts of distributed systems, consensus mechanisms, and decentralized applications (Khan, 2021). According to Latif (2021), using Truffle requires a basic understanding of the command line interface, JavaScript, and JSON. Additionally, you should be familiar with the process of deploying smart contracts on the Ethereum network (Patidar and Jain, 2019).

4.2 Flutter

Flutter is an open-source framework for mobile application development created by Google. The technology creates powerful cross-platform mobile apps using a single code base (Singh et al., 2022). Flutter uses the Dart programming language. The Dart programming language is a client-optimized language for fast apps on any platform. In this app, I use Flutter to create UI and front end of the application. Flutter offers a wide range of widgets and tools for creating beautiful and responsive mobile apps. Flutter also supports hot reload, which enables real-time code changes and aids in rapid app development (Singh et al., 2022). Using Flutter requires knowledge of the Dart programming language, object-oriented programming principles, and mobile app development. You should also be familiar with widgets, layouts, and state management (Singh et al., 2022).

4.3 Web3dart

Web3dart is a Dart library that provides a simple and easy-to-use API for connecting to Ethereum nodes and interacting with smart contracts. It allows our Flutter app to communicate with the smart contract deployed on the Ethereum network (Corradini *et al.,* 2022). Web3dart is built on top of the JSON-RPC API, which is a remote procedure call protocol used by Ethereum nodes. Web3dart simplifies the process of interacting with the Ethereum blockchain by providing a high-level API that abstracts away many of the low-level details of the JSON-RPC API (Corradini *et al.,* 2022). To use web3dart, one must have knowledge of the Ethereum blockchain, smart contracts, and the JSON-RPC API. Additionally, one must be familiar with the Dart programming language and asynchronous programming (Corradini *et al.,* 2022).

4.4 Model-View-Controller (MVC) Architecture

Model-View-Controller (MVC) architecture is a software design pattern that divides an application into three main components: Models, Views, and Controllers. Models represent data and business logic (Aini et al., 2022). The view represents the user interface and the controller acts as an intermediary between the two. The current application uses the MVC pattern to separate the various components of the application. Models are represented by smart contracts that store data and business logic. A view is represented by a UI built in Flutter. A controller is represented by the logic that connects the view to the model and handles user interactions. By using the MVC pattern, you can create a clean, maintainable code base that is easy to understand and change. To use the MVC pattern, one must have knowledge of software design patterns, object-oriented programming principles, and software architecture (Aini *et al.*, 2022). Overall, the implementation of the record-keeping app requires a combination of knowledge in blockchain technology, smart contract development, mobile app development, and software design patterns. By using these technologies and frameworks, it was possible to create a robust and reliable app that allows users to store and retrieve data on the Ethereum blockchain.

4.5 Python

Python is used in FastAPI web framework used for building APIs (Lathkar, 2023). It is known for its speed, ease of use, and documentation generation. One important feature of FastAPI is its built-in support for authentication. FastAPI provides several built-in authentication mechanisms such as OAuth2, HTTP Basic Auth, and JWT tokens (Lathkar, 2023). These mechanisms can be used to protect API endpoints from unauthorized access and ensure that only authenticated users can access certain resources. Bruce Schneier, a noted expert in the field of computer security, has emphasized the importance of authentication in securing computer systems. In his book, "Secrets and Lies: Digital Security in a Networked World," Schneier argues that authentication is a critical component of any security system, as it ensures that only authorized users are able to access sensitive resources (Schneier, 2000).

Ross Anderson, another prominent security researcher, has written extensively on the topic of authentication. In his paper, "Why Cryptography is Harder Than It Looks," Anderson highlights the challenges of implementing secure authentication systems and discusses the various approaches that have been used to address these challenges (Anderson, 2001).

Adam Shostack, a security consultant and author of "Threat Modeling: Designing for Security," has emphasized the importance of threat modeling in the design of secure authentication systems (Shostack, 2014). By carefully analyzing potential threats and vulnerabilities, developers can design authentication systems that are more resilient to attack.

5 Implementation

Blockchain technology has gained immense popularity in recent years due to its ability to provide secure and decentralized systems. This section focuses on the implementation of a blockchain app using Flutter, Solidity, and Truffle to build a record-keeping app. The main aim of this app is to provide a secure and transparent way to store and retrieve records.

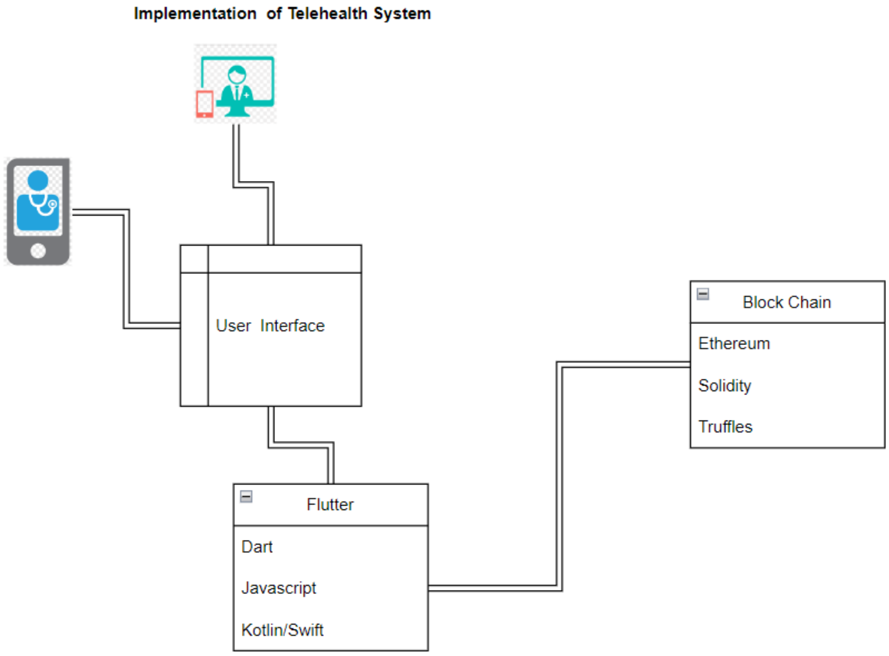

Figure 3: Implementation of telehealth system

Tools and Languages

From figure 3 above, there are three main concepts, the users' interface, flutter framework and blockchain network. Flutter is a popular mobile app development framework that has gained widespread popularity due to its unique features, ease of use, and fast development time. Flutter allows developers to build high-performance, visually appealing, and user-friendly interfaces for patients and doctors to access and manage their medical data (Aini *et al*., 2022). The framework provides a rich set of customizable widgets that enable developers to create dynamic and responsive user interfaces. Some of the key features of Flutter that make it an ideal choice for blockchain telehealth systems include its fast development time, hot reload feature, and customizable widgets. Flutter provides a wide range of pre-built widgets, including buttons, text fields, and sliders (Aini *et al*., 2022). These widgets can be customized and extended to create more complex UI elements that cater to the specific needs of a blockchain telehealth system. According to Imbugwa, Mazzara and Distefano (2020), Flutter's fast development time is another key advantage, as it allows developers to build, test, and deploy applications quickly. This feature is particularly important in a telehealth system, where rapid development is critical to meet the demands of patients and healthcare providers. Flutter's hot reload feature is another major advantage for developers building blockchain telehealth systems. This feature allows developers to make changes to the application's code while it is running, without needing to restart the app. This can save a significant amount of development time, as developers can instantly see the results of their code changes without needing to go through a lengthy build and deployment process (Imbugwa, Mazzara and Distefano, 2020).

Ethereum is a popular blockchain platform that can be used to build blockchain telehealth systems. Ethereum provides a secure and decentralized platform for building applications that require trust and transparency. Ethereum is particularly well-suited for building blockchain telehealth systems due to its smart contract functionality, which allows developers to automate the process of storing, managing, and sharing patient data (Wang *et al.* 2021).

Solidity is the programming language used to write smart contracts on the Ethereum blockchain. Solidity is a contract-oriented programming language that is designed to run on the Ethereum Virtual

Machine (EVM) (Aini *et al*., 2022). Solidity allows developers to write complex smart contracts that can automate the process of managing patient data. Smart contracts can be used to ensure that patient data is stored securely, and that only authorized parties have access to it (Khan, 2021). Smart contracts can also be used to manage patient consent, ensure the accuracy of patient data, and automate the process of payment between patients and healthcare providers.

Truffle is a development framework that provides tools and libraries for building, testing, and deploying smart contracts (Aini *et al*., 2022). Truffle simplifies the process of building decentralized applications (dApps) on the Ethereum blockchain, by providing a set of pre-built tools and libraries that enable developers to build and deploy smart contracts quickly and easily. Truffle includes a suite of tools for testing smart contracts, including a testing framework and a debugger. Truffle also provides tools for deploying smart contracts to the Ethereum blockchain, including a migration framework that automates the process of deploying smart contracts (Khan, 2021).

Overall, Flutter, Ethereum, Solidity, and Truffle are powerful tools for building blockchain telehealth systems that are secure, reliable, and user-friendly. These tools can be used to create a seamless and transparent platform for storing and managing patient data, enabling patients and healthcare providers to access and share medical data securely and efficiently. As the demand for telehealth services continues to grow, the use of blockchain technology is likely to become increasingly important in ensuring the security and privacy of patient data.

6 Evaluation

The blockchain app built using Flutter, Solidity, and Truffle for storing and sharing records provides a valuable case study for understanding the potential of blockchain technology for secure and decentralized record-keeping. This analysis examines the main results and findings of the study, as well as the implications of these findings from both an academic and practitioner perspective.

6.1 Experiment 1: How can blockchain technology facilitate updating healthcare data in the online database?

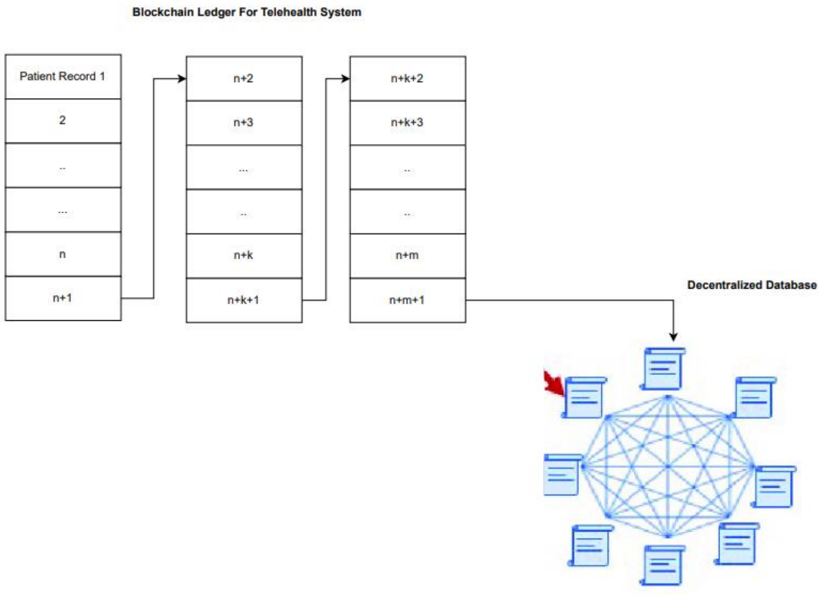

Figure 4: Blockchain ledger for telehealth system

In a blockchain telehealth system, medical records are added to the blockchain using a process called "hashing." Hashing is a mathematical process that takes a block of data and creates a unique digital fingerprint, known as a hash, that is specific to that data (Sheth and Dattani, 2019). The hash is then stored on the blockchain, along with a timestamp and a reference to the previous block in the chain, creating an immutable record that cannot be altered or deleted as shown in the figure 4 above. To add a medical record to the blockchain in a telehealth system, the following steps are typically taken:

i. Data Entry: The doctor enters the medical record information into a digital form or interface.
ii. Hashing: The medical record information is then processed through a hashing algorithm, which generates a unique digital fingerprint (hash) for the record.
iii. Digital Signature: The hash is then signed using a digital signature, which verifies the identity of the person adding the record and ensures the integrity of the data.
iv. Record Creation: The signed hash is added to a new block on the blockchain, along with a timestamp and a reference to the previous block in the chain, creating an immutable record of the medical information.
v. Verification: Once the record is added to the blockchain, it is verified by other nodes in the network to ensure its accuracy and integrity.
vi. Storage: The record is stored on the blockchain, where it can be accessed securely by authorized parties, such as doctors or patients, using their private keys

By adding medical records to the blockchain in this way, a telehealth system can ensure the security, integrity, and privacy of patient data. The use of hashing and digital signatures provides a secure and transparent way to store and share medical information, while the decentralized nature of the blockchain ensures that the data cannot be altered or deleted without the consensus of the network (Sheth and Dattani, 2019). This makes blockchain technology an ideal solution for telehealth systems, where data security and privacy are critical.

From the figure above, each block of records is linked to the previous block in the chain through a cryptographic hash function, creating a tamper-proof and transparent record of all transactions in the network. This linking process is known as "chaining" or "blockchain linking." The linking process is as follows:

i. A block of records is created: Each block in the chain contains a group of records or transactions, such as medical records or patient data. These records are validated and then stored in the block.
ii. A hash is generated: Once the records are stored in the block, a unique cryptographic hash is generated using a hashing algorithm. This hash is like a digital fingerprint that uniquely identifies the block of records.
iii. The hash is added to the block as a header, along with a timestamp and other metadata.
iv. The block is linked to the previous block: To create the chain, the hash of the previous block in the chain is added to the header of the current block. This links the two blocks together, creating a chain of blocks that is tamper-proof and transparent.
v. The block is added to the blockchain: Once the current block is linked to the previous block, it is added to the blockchain, a decentralized ledger that is maintained by all nodes in the network. This ensures that the block is immutable and cannot be altered or deleted without consensus from the network.

By linking each block of records to the previous block in the chain, the blockchain telehealth system creates a tamper-proof and transparent record of all transactions in the network. This ensures that all records are validated, secure, and cannot be altered or deleted without the consensus of the network (Sheth and Dattani, 2019). Additionally, this linking process provides a mechanism for tracing the history of each record, allowing healthcare providers to track the progress of a patient's care over time.

In the system developed, the underlying ledger is powered by Solidity. Ledgers are an essential component of blockchain technology and play an important role in the creation of immutable records. A blockchain-based ledger is immutable because each block in the chain contains a cryptographic hash of the previous block's data as discussed by Parameswari and Mandadi (2020). This means that any change to the data in a previous block necessitates updating the hash in subsequent blocks in the chain. Furthermore, because blockchain networks are decentralized, each node on the network keeps a copy of the ledger. This makes it extremely difficult for an attacker to tamper with the data in the ledger because they would have to modify the data on all copies of the ledger at the same time, which is nearly impossible (Parameswari and Mandadi, 2020). Furthermore, the process of adding a new block to the chain includes a consensus mechanism that ensures that all nodes on the network agree on the new block's validity. Because a malicious actor would need to control a majority of the nodes on the network to introduce invalid data into the network, this consensus mechanism makes it extremely difficult for them to do so (Panda and Satapathy, 2021). The following steps are necessary to achieve blockchain technology that facilitates updating healthcare data in the online database.

Steps for Experiment 1

1. **Create a transaction**

The first step is to create a transaction that specifies the details of the transaction. This includes the sender's address, the recipient's address, the amount being transferred, and any additional data that is required (Morkunas *et. al.*, 2019). In this case, the sender will be the doctor and the patient, recipient is the distributed database, and the data includes the patient's information.

2. **Verify the transaction**

Once the transaction is created, it needs to be verified to ensure that it is valid. This involves checking that the sender is authorized to make the transaction, that the recipient's address is valid, and that the transaction conforms to the rules of the blockchain protocol. This can be seen through the doctor's and patient's login to their Solidity account.

3. **Broadcast the transaction**

Once the transaction is verified, it needs to be broadcast to the network. This involves sending the transaction to other nodes on the network, which will then validate the transaction and add it to their copy of the ledger. The Solidity framework distributes the block across the different databases (Javaid *et al*, 2021).

4. **Mining**

In order to add the transaction to the ledger, it needs to be added to a block. This involves miners using their computing power to solve a complex mathematical puzzle which adds the block to the blockchain and earns the miner a reward. The Ethereum blockchain contains a network of miners that ensures a block goes through verification through complex mathematical computation.

5. **Adding the block to the chain**

Once the block has been mined, it needs to be added to the blockchain (Morkunas *et al*., 2019). This involves other nodes on the network validating the block and adding it to their copy of the ledger.

6. **Updating the ledger**

Once the block has been added to the blockchain, the ledger is updated with the new transaction. Blockchain technology can facilitate the updating of healthcare data in online databases and hence leading to different positive outcomes. For instance, Hasan *et al.* (2021) wrote that Blockchain technology facilitates secure and transparent data sharing among authorized parties since it ensures that all transactions are validated and recorded in a tamper-proof and transparent manner, eliminating the need for intermediaries and reducing the risk of data breaches or fraud. Besides, the scholars observed that blockchain technology improves data accuracy and integrity since smart contracts ensure that data is validated, authenticated, and stored securely, reducing the risk of errors, omissions, or unauthorized modifications. In addition, blockchain facilitates faster and more efficient data exchange since the peer-to-peer network, blockchain technology eliminates the need for intermediaries, reducing transaction costs and delays

6.2 Experiment 2: How can blockchain technology help to enhance data integrity and privacy in setups where the ledger is shared

The application developed in this project uses Ethereum based system. Ethereum is a blockchain platform that enables developers to build decentralized applications using smart contracts. One of the key features of Ethereum is its ability to create and deploy new tokens on the network, known as ERC-20 tokens (Hasan *et al.,* 2021). With the help of Ethereum architecture, blockchain technology can enhance data integrity and privacy in setups where the ledger is shared by providing several mechanisms that ensure the authenticity, immutability, and confidentiality of data. Blockchain technology uses digital signatures to ensure the authenticity of data (Khandelwal, 2021). Digital signatures use cryptographic algorithms to create a unique signature for each transaction. These signatures are verified by the network to ensure that only authorized parties can modify or access the data ensuring data remains secure and authentic. Blockchain technology can use encryption to ensure the confidentiality of data. By encrypting data, blockchain technology ensures that only authorized parties can access the data, even when it is shared across multiple parties. Blockchain technology uses consensus mechanisms to ensure that all parties on the network agree on the validity of transactions. This consensus mechanism helps to prevent malicious actors from modifying or introducing invalid data into the network (Abd-Alrazaq *et al*., 2021). The following steps are necessary to enable a blockchain technology that enhances data integrity and privacy in setups where the ledger is shared.

Steps for Experiment 2

i. Permission access: The doctor and patient should have a valid ID
ii. Anonymous transaction: The transaction carried out by doctors and patients are anonymous. These transactions are only recognized via their unique ID.
iii. Immutable records. Once the block has been added to the ledger they cannot be changed.
iv. Consensus Algorithm. Ensure that the algorithm used for mining uses the same mathematical algorithm (BouSaba and Anderson, 2019).

The experiment demonstrates that blockchain technology can help to enhance data integrity and privacy in telehealth systems. Abd-Alrazaq *et al*. (2021) wrote that blockchain technology creates an immutable and tamper-proof record of all transactions on the network. This ensures that all healthcare data recorded on the blockchain is secure, accurate, and verifiable, reducing the risk of data breaches, fraud, and errors. Similarly, blockchain uses encryption and digital signatures to ensure that only authorized parties can access and update healthcare data. Encryption ensures that data is securely stored and transmitted, while digital signatures provide a way to authenticate transactions and ensure that only authorized parties can modify data. This enhances data privacy and ensures that healthcare data remains confidential and protected.

7 Conclusion

Blockchain applications are becoming increasingly popular for their ability to provide secure, decentralized storage and sharing of data. The project was aimed at creating a blockchain app that could provide secure and decentralized storage and sharing of records using the Ethereum blockchain. The app was developed using Flutter, a mobile app development framework, which allowed for the creation of both Android and iOS versions of the app. Solidity, a programming language used for developing smart contracts on the Ethereum blockchain, was used to write the smart contracts that enabled the storage and sharing of records on the blockchain. Truffle, a development environment and testing framework for Ethereum-based applications, was used to help with the development and deployment of the smart contracts. The app had several features that enabled users to create an account and store their records on the Ethereum blockchain. The app used the MetaMask wallet to interact with the Ethereum blockchain and to pay for the gas fees associated with executing transactions on the network.

Overall, the findings from this project demonstrate the potential of using Flutter, Solidity, and Truffle to build blockchain applications for secure record storage and sharing. While there are some challenges associated with using blockchain technology, the benefits of security and decentralization make it an attractive option for many user cases.

8 Future Work

There are a number of potential risks and challenges associated with using telehealth systems that must be addressed before telehealth systems can be effectively implemented (Haleem *et al*, 2021). These include ensuring patient privacy and security, ensuring quality of care, and ensuring cost-effectiveness and cost-savings. It is also important to consider the most effective ways of utilizing these systems and the best practices for implementing them in different settings. In order to maximize the potential of telehealth systems, there is a need for further research and development (Siyal, 2019). This includes developing more advanced and secure telehealth systems that are tailored to specific medical conditions, exploring the use of artificial intelligence and machine learning to improve telehealth systems, investigating the potential of using virtual reality and augmented reality in telehealth systems, creating a telehealth platform that supports real-time communication between healthcare providers and patients, and developing guidelines.

9 References

Abd-Alrazaq, A. A., Alajlani, M., Alhuwail, D., Erbad, A., Giannicchi, A., Shah, Z., ... & Househ, M. (2021). Blockchain technologies to mitigate COVID-19 challenges: A scoping review. *Computer methods and programs in biomedicine update*, *1*, 100001.

Afreen, N., Khatoon, A. and Sadiq, M. (2016). A taxonomy of software's non-functional requirements. In *Proceedings of the second international conference on computer and communication technologies* (pp. 47-53). Springer, New Delhi.

Ahmad, R.W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S. and Omar, M. (2021). The role of blockchain technology in telehealth and telemedicine. *International journal of medical informatics*, *148*, p.104399.

Aini, Q., Budiarto, M., Putra, P. O. H., & Santoso, N. P. L. (2020). Lecturer certification management using blockchain technology. *Journal of Advanced Research in Dynamical and Control Systems*, *12*(6), 624-631.

Anderson, R. (2001). Why Cryptography is Harder Than It Looks. In Advances in Cryptology - EUROCRYPT 2001 (pp. 1-18). Springer Berlin Heidelberg.

Awad, A., *et al*., (2021). "MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange," in *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15762-15775, 1 Nov.1, 2021, doi: 10.1109/JIOT.2021.3052910

Azaria, A. Ekblaw, T. Vieira and A. Lippman, (2016). "MedRec: Using Blockchain for Medical Data Access and Permission Management," *2016 2nd International Conference on Open and Big Data (OBD)* pp. 25-30, doi: 10.1109/OBD.2016.11.

Balcerzak, A. P., Nica, E., Rogalska, E., Poliak, M., Klieštik, T., & Sabie, O. M. (2022). Blockchain technology and smart contracts in decentralized governance systems. *Administrative Sciences*, *12*(3), 96.

Bhanushali, D., Koul, A., Sharma, S. and Shaikh, B., (2020). BlockChain to Prevent Fraudulent Activities: Buying and Selling Property Using BlockChain. In *2020 International Conference on Inventive Computation Technologies (ICICT)* (pp. 705-709). IEEE.

BouSaba, C., & Anderson, E. (2019). Degree validation application using solidity and Ethereum blockchain. In *2019 SoutheastCon* (pp. 1-5). IEEE.

Chakraborty, S., Aich, S. and Kim, H.C., (2019). A secure healthcare system design framework using blockchain technology. In *2019 21st International Conference on Advanced Communication Technology (ICACT)* (pp. 260-264). IEEE.

Charanya, R. and Aramudhan, M. (2016). Survey on access control issues in cloud computing. In *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)* (pp. 1-4). IEEE.

Corradini, F., Marcelletti, A., Morichetta, A., Polini, A., Re, B., & Tiezzi, F. (2022). A Choreography-Driven Approach for Blockchain-Based IoT Applications. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)* (pp. 255-260). IEEE.

Demertzis, K., Kikiras, P. and Iliadis, L., (2022). A Blockchained Secure and Integrity-Preserved Architecture for Military Logistics Operations. In *International Conference on Engineering Applications of Neural Networks* (pp. 271-283). Springer, Cham.

Devi Parameswari, C., & Mandadi, V. (2021). Public distribution system based on blockchain using solidity. In *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2020* (pp. 175-183). Springer Singapore.

Drago, C., Gatto, A., & Ruggeri, M. (2021). Telemedicine as technoinnovation to tackle COVID-19: A bibliometric analysis. *Technovation*, 102417.

Durneva, P., Cousins, K. and Chen, M. (2020). The current state of research, challenges, and future research directions of blockchain technology in patient care: systematic review. *Journal of medical Internet research*, *22*(7), p.e18619.

Eastman, P., Swails, J., Chodera, J.D., McGibbon, R.T., Zhao, Y., Beauchamp, K.A., Wang, L.P., Simmonett, A.C., Harrigan, M.P., Stern, C.D. and Wiewiora, R.P. (2017). OpenMM 7: Rapid development of high-performance algorithms for molecular dynamics. *PLoS computational biology*, *13*(7), p.e1005659.

Ebbesen, M., Sørensen, K.D., Pedersen, B.G. and Andersen, S. (2022). Ethical Principles in the Analysis of Prostate Cancer Diagnostics. *Cancer Investigation*, (just-accepted), pp.1-15

Faragardi, H.R. (2017). Ethical considerations in cloud computing systems. *Multidisciplinary Digital Publishing Institute Proceedings*, *1*(3), p.166.

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, *2*, 130-139.

Hasan, H. R., Salah, K., Jayaraman, R., Yaqoob, I., Omar, M., & Ellahham, S. (2021). Blockchain-enabled telehealth services using smart contracts. *Ieee Access*, *9*, 151944-151959.

He, L., Madathil, S. C., Oberoi, A., Servis, G., & Khasawneh, M. T. (2019). A systematic review of research design and modeling techniques in inpatient bed management. *Computers & Industrial Engineering*, *127*, 451-466.

Hercigonja, Z., (2016). Comparative analysis of cryptographic algorithms. *International Journal of Digital Technology & Economy*, *1*(2), pp.127-134.

Imbugwa, G., Mazzara, M., & Distefano, S. (2020). Developing a mobile application using open-source parking management system on etherium smart contracts. In *Journal of Physics: Conference Series* (Vol. 1694, No. 1, p. 012022). IOP Publishing.

Jain, S., Ahuja, N.J., Srikanth, P., Bhadane, K.V., Nagaiah, B., Kumar, A. and Konstantinou, C., (2021). Blockchain and autonomous vehicles: recent advances and future directions. *IEEE Access*.

Javaid, M., Haleem, A., Singh, R. P., Khan, S., & Suman, R. (2021). Blockchain technology applications for Industry 4.0: A literature-based review. *Blockchain: Research and Applications*, *2*(4), 100027.

Khan, Shafaq Naheed, et al. "Blockchain smart contracts: Applications, challenges, and future trends." *Peer-to-peer Networking and Applications* 14 (2021): 2901-2925.

Khandelwal, P., Johari, R., Gaur, V., & Vashisth, D. (2021). BlockChain Technology based Smart Contract Agreement on REMIX IDE. In *2021 8th International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 938-942). IEEE.

Kumar, R. and Tripathi, R. (2019). Traceability of counterfeit medicine supply chain through Blockchain. In *2019 11th international conference on communication systems & networks (COMSNETS)* (pp. 568-570). IEEE.

Lathkar, M. (2023). Getting Started with FastAPI. In *High-Performance Web Apps with FastAPI: The Asynchronous Web Framework Based on Modern Python* (pp. 29-64). Berkeley, CA: Apress.

Latif, R. M. A., Farhan, M., Rizwan, O., Hussain, M., Jabbar, S., & Khalid, S. (2021). Retail level Blockchain transformation for product supply chain using truffle development platform. *Cluster Computing*, *24*, 1-16.

Ledyard, J.O., (2020). of Experimental Research. *The handbook of experimental economics*, p.111.

Linke, N.M., Maslov, D., Roetteler, M., Debnath, S., Figgatt, C., Landsman, K.A., Wright, K. and Monroe, C., (2017). Experimental comparison of two quantum computing architectures. *Proceedings of the National Academy of Sciences*, *114*(13), pp.3305-3310.

Madir, J., (2019). Blockchain in healthcare: a Panacea or Scourge. *Available at SSRN 3475632*.

Maheshwari, S., Raychaudhuri, D., Seskar, I. and Bronzino, F. (2018). Scalability and performance evaluation of edge cloud systems for latency constrained applications. In *2018 IEEE/ACM Symposium on Edge Computing (SEC)* (pp. 286-299). IEEE.

Mannaro, & Ibba, S. (2018). A blockchain approach applied to a teledermatology platform in the Sardinian region (Italy). *Information*, *9*(2), 4.

Mingxiao, D., Xiaofeng, M., Zhe, Z., Xiangwei, W. and Qijun, C. (2017). A review on consensus algorithm of blockchain. In *2017 IEEE international conference on systems, man, and cybernetics (SMC)* (pp. 2567-2572). IEEE.

Mohammed, T. J., Albahri, A. S., Zaidan, A. A., Albahri, O. S., Al-Obaidi, J. R., Zaidan, B. B., ... & Hadi, S. M. (2021). Convalescent-plasma-transfusion intelligent framework for rescuing COVID-19 patients across centralised/decentralised telemedicine hospitals based on AHP-group TOPSIS and matching component. *Applied Intelligence*, *51*(5), 2956-2987.

Morkunas, V. J., Paschen, J., & Boon, E. (2019). How blockchain technologies impact your business model. *Business Horizons*, *62*(3), 295-306.

Panda, S. K., & Satapathy, S. C. (2021). An investigation into smart contract deployment on Ethereum platform using Web3. js and solidity using blockchain. In *Data Engineering and Intelligent Computing: Proceedings of ICICC 2020* (pp. 549-561). Springer Singapore.

Parameswari, C. D., & Mandadi, V. (2020). Healthcare data protection based on blockchain using solidity. In *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)* (pp. 577-580). IEEE.

Patidar, K., & Jain, S. (2019). Decentralized e-voting portal using blockchain. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.

Rui, H., Huan, L., Yang, H. and YunHao, Z., (2020). Research on secure transmission and storage of energy IoT information based on Blockchain. *Peer-to-Peer Networking and Applications*, *13*(4), pp.1225-1235.

Schneier, B. (2000). Secrets and lies: digital security in a networked world. Wiley.

Sharma, V., Gupta, A., Hasan, N.U., Shabaz, M. and Ofori, I. (2022). Blockchain in Secure Healthcare Systems: State of the Art, Limitations, and Future Directions. *Security and Communication Networks*, *2022*

Sheth, H., & Dattani, J. (2019). Overview of blockchain technology. *Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146*.

Shu, Z. and G. Yan. (2022) "IoTInfer: Automated Blackbox Fuzz Testing of IoT Network Protocols Guided by Finite State Machine Inference," in *IEEE Internet of Things Journal*, doi: 10.1109/JIOT.2022.3182589

Singh, A. V., Tiwari, A. O., Singh, S. S., & Lobo, V. B. (2022). A Criminal Record Keeper System using Blockchain. In *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 840-845). IEEE.

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography*, *3*(1), 3.

Shostack, A. (2014). Threat modeling: designing for security. John Wiley & Sons.

Si, H., Sun, C., Li, Y., Qiao, H. and Shi, L. (2019). IoT information sharing security mechanism based on blockchain technology. *Future Generation Computer Systems*, *101*, pp.1028-1040.

Sosu, R.N.A., Quist-Aphetsi, K. and Nana, L., (2019). A decentralized cryptographic blockchain approach for health information system. In *2019 International Conference on Computing, Computational Modelling and Applications (ICCMA)* (pp. 120-1204). IEEE.

Temesgen, Z. M., DeSimone, D. C., Mahmood, M., Libertin, C. R., Palraj, B. R. V., & Berbari, E. F. (2020). Health care after the COVID-19 pandemic and the influence of telemedicine. In *Mayo Clinic Proceedings* (Vol. 95, No. 9, pp. S66-S68). Elsevier.

Todaro, J.M., (2020). Overview of MedCredits. *online, accessed*, *6*(05), p.2020.

Wang, Z., Jin, H., Dai, W., Choo, K. K. R., & Zou, D. (2021). Ethereum smart contract security research: survey and future research opportunities. *Frontiers of Computer Science*, *15*, 1-18.

Xenya, M.C. and Quist-Aphetsi, K., (2019). Decentralized distributed blockchain ledger for financial transaction backup data. In *2019 International Conference on Cyber Security and Internet of Things (ICSIoT)* (pp. 34-36). IEEE.

Yue, Y. and X. Fu (2021) "Research on Medical Equipment Supply Chain Management Method Based on Blockchain Technology," *2020 International Conference on Service Science (ICSS)*, 2020, pp. 143-148, doi: 10.1109/ICSS50103.2020.00030

Zhang, J. "Ethical Issues in Information Systems," *2011 International Conference of Information Technology, Computer Engineering and Management Sciences*, 2011, pp. 321-323, doi: 10.1109/ICM.2011.24

Zhang, P. and Boulos, M.N.K., 2020. Blockchain solutions for healthcare. In *Precision Medicine for Investigators, Practitioners and Providers* (pp. 519-524). Academic Press.