“Blockchain Technology in Healthcare System”

A PROJECT REPORT

SUBMITTED IN THE PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE AWARD OF DEGREE

OF

MASTER OF TECHNOLOGY

IN

SOFTWARE ENGINEERING

Submitted By

Harshil Lalka

(2k21/SWE/11)

Under the supervision of

Dr. Abhilasha Sharma

Assistant Professor

Department of Software Engineering

Delhi Technological University, Delhi

Department of Software Engineering

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Bawana Roas, Delhi-110042

MAY-2023

DECLARATION

I, **Harshil Lalka, 2k21/SWE/11** student of **M.tech (SWE)**, hereby declare that the project entitled **"Blockchain Technology in Healthcare system"** is submitted by me to the Department of Software Engineering, **Delhi Technological University**, Shahbad Daulatpur, Delhi. I have done my project in partial fulfilment of the requirement for the award of the degree of Master of Technology in Software Engineering and it has not been previously formed the basis for any fulfilment of the requirement in any degree or other similar title or recognition. This report is an authentic record of my work carried out during my degree under the guidance of **Dr. Abhilasha Sharma.**

Place: Delhi **Harshil Lalka**

Date: 29th May,2023 **(2K21/SWE/11)**

CERTIFICATE

I hereby certify that the project entitled **"Blockchain Technology in Healthcare System"** which is submitted by Harshil Lalka (2K21/SWE/11) to the Department of Software Engineering, Delhi Technological University, Shahbad Daulatpur, Delhi in partial fulfilment of the requirement for the award of the degree of Master of Technology in Software Engineering, is a record of the project work carried out by the student under my supervision.

Place: Delhi
Date: 29th May, 2023

Dr. Abhilasha Sharma
SUPERVISOR
Assistant Professor,
Department of Software Engineering

ACKNOWLEDGEMENT

I am very thankful to **Dr. Abhilasha Sharma** (Assistant Professor, Department of Software Engineering) and all the faculty members of the Department of Software engineering at DTU. They all provided us with immense support and guidance for the project.

I would also like to express my gratitude to the University for providing us with the laboratories, infrastructure, testing facilities and environment which allowed us to work without any obstructions.

I would also like to appreciate the support provided to us by our lab assistants, seniors and our peer group who aided us with all the knowledge they had regarding various topics.

Harshil Lalka
(2K21/SWE/11)

ABSTRACT

Blockchain technology has come out as a promising solution to address the persistent challenges of data security, privacy, and interoperability in the healthcare industry. This thesis explores the application of blockchain technology in healthcare to improve data management, enhance patient privacy, and facilitate seamless data exchange among medical facilities.

The research begins with an indepth analysis of data challenges in the healthcare system, including data fragmentation, silos, security breaches, and lack of interoperability. It establishes the need for a robust and secure infrastructure to overcome these challenges and proposes blockchain as a potential solution.

The thesis investigates the fundamental concepts and principles of blockchain technology, including decentralization, immutability, consensus mechanisms. It explores blockchain architectures and consensus algorithms to identify the most suitable approach for the healthcare domain.

Furthermore, the research develops into the specific use cases of blockchain in medical industry, such as secure patient data management, interoperability across EHR systems, clinical research data sharing, and drug supply chain management. Each use case is analyzed in terms of its potential benefits, implementation challenges, and impact on stakeholders.

To evaluate the feasibility and effectiveness of blockchain technology in the healthcare system, the thesis presents a proof-of-concept implementation. A blockchain-based platform is developed and tested, demonstrating its ability to enhance data security, privacy, and interoperability in a real-world healthcare environment.

Lastly, the thesis discusses the limitations and future research directions of blockchain technology in healthcare. It highlights potential scalability challenges, the need for standardization, and the importance of user acceptance and adoption.

In conclusion, this thesis establishes the potential of blockchain technology to address the data challenges in the healthcare system. It provides valuable insights for healthcare practitioners, policymakers, and researchers on blockchain for secure and interoperable data management, paving the way for a more efficient and patient-centric healthcare ecosystem.

CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

Abbreviations	Full form
DPoS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
DApps	Decentralized applications
ICO	Initial Coin Offerings
ECDSA	Elliptic Curve Digital Signature Algorithm
HIPAA	Health Insurance Portability and Accountability Act

CHAPTER 1
INTRODUCTION

1.1 Blockchain

Blockchain is one of the leading technologies in the world. With the increase in the vulnerability to the data, blockchain is being adopted by major organizations to strengthen their security for the shareable data. Reason behind adopting blockchain is its inherent security qualities. Three principles of blockchain which insures trust in transactions are consensus algorithm, cryptography, and decentralization. Blockchain which was initially used in the field of finance but now is spreading to different sectors, and one of the sectors where blockchain has an immense potential is healthcare.

At its core, a blockchain is a digital ledger or a distributed database that maintains a growing list of records called blocks. Each block contains data or a set of transactions, along with a unique identifier called a cryptographic hash, which ensures the integrity and immutability of the block. These blocks are linked together, forming a chain of blocks, hence the name "blockchain."

1.2 Important Terminologies in Blockchain

1.2.1 Decentralization

Decentralization is one of the main principal of blockchain which gives it a uphand over the existing centralized technologies. Unlike the centralized technologies where the control is with one authority and data manipulation can be done easy, in blockchain data is distributed among all participants or nodes. Each node in the network which can be spread over the world has a copy of the entire blockchain and they all must reach consensus to add a block of data to the network.

1.2.2 Consensus mechanisms

Base of decentralization in blockchain is the consensus mechanism that it follows. Blockchain requires agreement from participants in the network to validate the transaction and the order in which it should be added. It ensures that even if malicious nodes are present the network the integrity of transaction added in maintained. Different blockchains have different methods of implementing consensus mechanism, some of the common consensus mechanisms are:

a) Proof of Work (PoW)

Bitcoin which is the first application of blockchain used "Proof of Work" as the consensus mechanism. It requires participants to solves complex puzzle to validate the transaction and add the block to the network. This consensus mechanism requires a good amount computation power and energy resource. The participants who solves the puzzle correctly are reward with newly created cryptocurrency like bitcoin. The nature of POW to be computationally expensive makes it hard to alter data in blockchain.

b) Proof of Stack (PoS)

The limitation of Proof of work of consuming a good amount of energy led us to explore alternate method to achieve consensus like proof of stack. Proof of stack chooses validators based on the stack that they have i.e. the cryptocurrency that they hold and stack in the network. Instead of solving puzzles, validators are selected randomly or in a deterministic manner based on their stake, and they take turns proposing and validating blocks. Validators who have a larger stake in the network have a higher chance of being selected.

c) Delegated Proof of Stake (DPoS)

DPoS is an extension of the PoS consensus mechanism that introduces a representative system. In DPoS, token holders vote for a limited number of delegates who are responsible for validating and producing blocks. These

delegates take turns in producing blocks in a round-robin manner. DPoS aims to increase transaction throughput by reducing the number of participants involved in block production, as well as improving scalability and efficiency. However, DPoS introduces a level of centralization, as the power to validate transactions and produce blocks lies in the hands of a limited number of delegates.

d) Proof of Authority (PoA)

PoA is a consensus mechanism that relies on a set of known and trusted validators or authorities to create blocks and validate transactions. Validators are typically chosen based on their reputation, identity, or the stake they hold. PoA is commonly used in private or consortium blockchains, where trust among participants is established beforehand. It offers fast transaction confirmation times and high scalability but sacrifices the decentralized nature of public blockchains.

e) Practical Byzantine Fault Tolerance (PBFT)

When the nodes are fixed then practical byzantine fault tolerance algorithm helps in providing fast consensus. It is specially designed for networks with permissioned blockchain. The nodes in this network act as validators or they can also be referred as replicas. A block is proposed by a replica and is sent to other replicas this phase is known as pre-prepare phase which is the phase one out 2 phase process in PBFT. In the next phase which is commit phase replicas agree on a particular block. Thus this replicas interchange message in order to reach a consensus to decide the order of blocks.

1.2.3 Smart Contracts

Smart contracts are implemented using programming languages specifically designed for creating them, such as Solidity for Ethereum. The code of a smart contract specifies the conditions, rules, and actions that will be carried out when those conditions are

met. Once the smart contract is deployed to the blockchain, it becomes immutable and cannot be altered, ensuring the integrity and reliability of the contract.

1.2.4 Distributed Ledger Technology (DLT)

Distributed Ledger Technology (DLT) is a type of database that enables multiple participants to share and maintain a decentralized record of transactions or information across a network. Blockchain is the most prominent and widely known implementation of this technology. Blockchain is a specific type of DLT that organizes and records data in a sequential chain of blocks. In a blockchain-based DLT system, transactions or data are grouped into blocks, which are then linked together in a chronological order.

CHAPTER 2
ARCHITECTURE OF BLOCKCHAIN

Architecture of blockchain allow nodes or computers to be connected to each other rather than a central server to share information. This design allow blockchain to create a distributed network where each node act as the administrator of this distributed network. Eliminating the central server or central authority allow the network to be more secure and less manipulative. Blockchain as the name suggests adopts a linked list type of nature like chain of blocks to store information. Financial transactions or data is stored in blocks which have a fixed structure, are linked to each other by each block storing the hash of the parent / previous block.

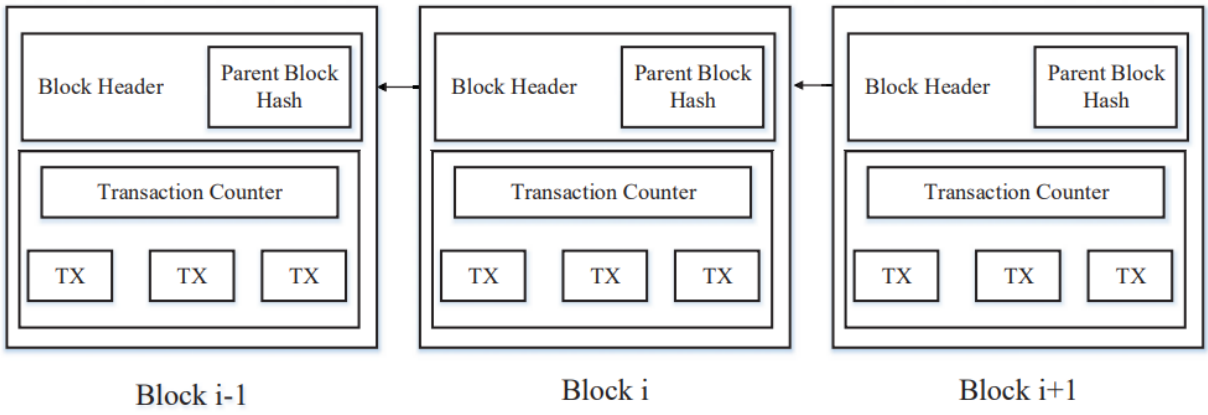

Fig.1: Blockchain Architecture

2.1 Components

2.1.1 Blocks

Blockchain maintains a series of block to store data. To maintain the linking between the blocks, all blocks store the hash of the parent block thus point to the previous block maintaining a link. First which does not have a parent to point to is known as genesis block. Each block has its unique identity defined by the hash which is defined when

the block is created. Any change in the data of the block will reflect by change in the hash of the block. Thus change in data of any form will reflect in the mismatch of current blocks hash in the next block thus breaking the chain. This property makes data in blockchain secure and immutable. A block being the main component of the blockchain architecture consists of `block header` and `block body`, the representation of the block is shown in the figure below. The header of the block consist of following fields:

a) Block version
b) Merkle tree root hash
c) Timestamp
d) nBits
e) Nounce
f) Parent Block Hash

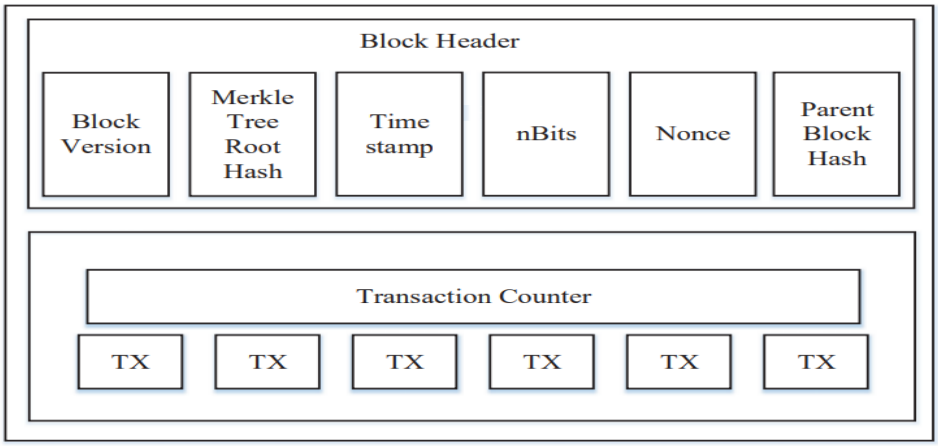

Fig.2: Block Structure

2.1.2 Digital Signature

Each node or user has private key and public key in the network. Private key allow user to sign the transaction which then is broadcasted in the network whereas the private key is kept confidential. Any with the public key can of the particular user can access the data of the transaction. But the access of transaction in the network to

anyone with the users public key creates a concern for confidentiality. Thus 2 layer encryption is done on the transaction before broadcasting the signed transaction in the network. If A wants to send data to B then first A will sign the transaction with its private key thus encrypting it to maintain authenticity that the data is sent by A, now to maintain the confidentiality the transaction that was signed by A's private key is again encrypted by B's public key so that the data can only be access with B's private key. This 2 layer encryption helps to maintain authenticity and confidentiality. And the common encryption algorithm used by blockchain is elliptic curve digital signature algorithm (ECDSA).

2.1.3 Merkle Tree

A block in a blockchain contains multiple transactions and now to maintain the integrity of data in blocks, hash of each block is stored in the header. To compute the hash of the block, hash of all transactions are calculated and computed into a single hash value using the hashing method of merkle tree and then that single hash value is stored in the root of the block. Storing the hash value of each transaction is not feasible in terms of scalability therefore merkle tree is used to maintain integrity and keep data storage efficient in the blockchain. Merkle tree is computed by hashing the pair of hash values from leat of the tree and going upto the root. In the blockchain leaf of the merkle tree contains the hash value of each transaction in the block. The hash values are then computed recursively upto the root thus giving a single hash value that represents all the transactions in that block and is stored in the header.

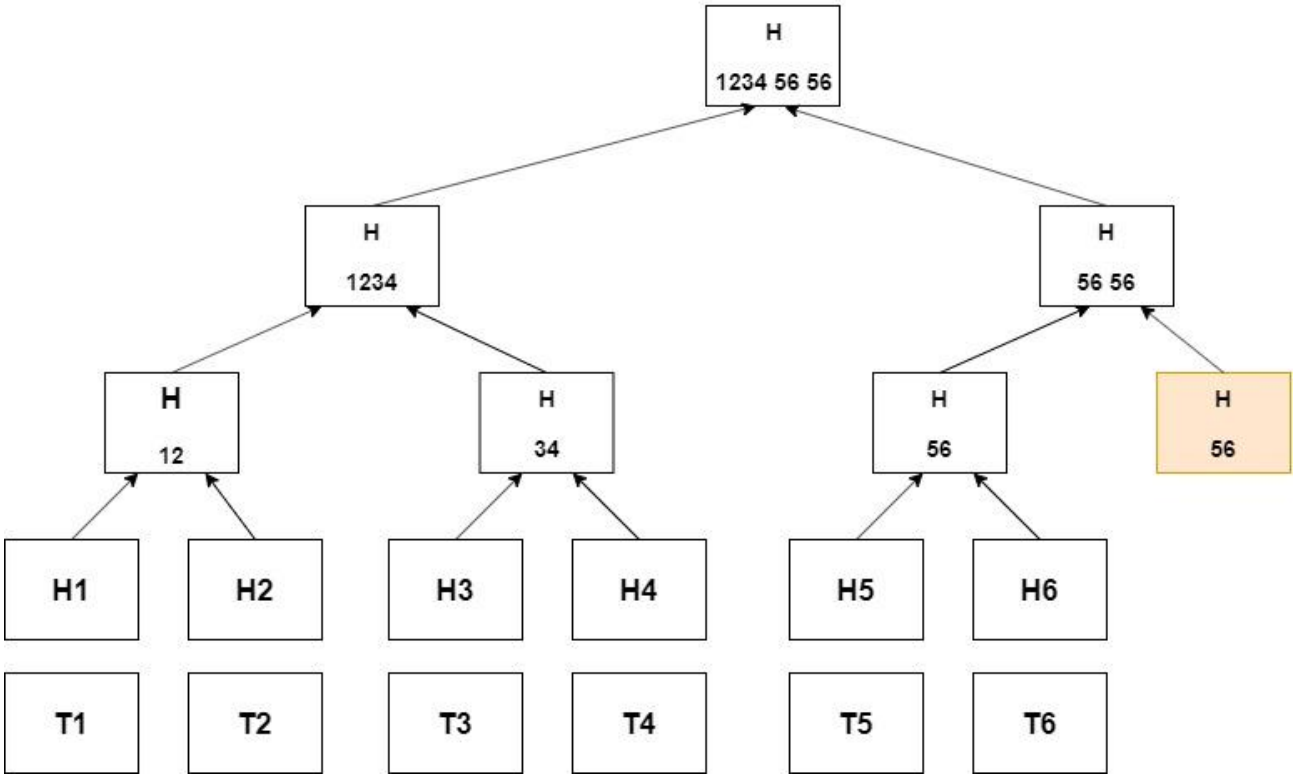

Fig.3: Merkle Hash Tree Representation

2.2 Public Blockchain vs Private Blockchain

2.2.1 Public Blockchain (Permissionless)

In public blockchain any node is allowed to join the network without any prior authentication and can validate blocks. Being the basic principals of blockchain decentralization is maintained in this blockchain thus removing any central authority. And to maintain agreement between nodes consensus mechanism is followed. All transactions and data on a public blockchain are transparent and visible to all participants. Anyone can inspect the blockchain's entire history, enhancing trust and accountability. Public blockchains utilize consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), to secure the network from attacks and maintain the integrity of the blockchain. Public blockchains often have a native cryptocurrency that serves as an incentive for participants (miners or validators) to maintain the network's operations and security.

2.2.2 Private Blockchain (Permissioned)

A private blockchain, also known as a permissioned blockchain, is a closed network where participation and access are restricted to selected entities or participants. It require permission to join and participate in the network. The network's creator or an appointed authority controls access, determining who can become a participant or node. Private blockchains often have a centralized entity or consortium that governs the network's rules, operations, and access permissions. This allows for greater control and faster decision-making compared to public blockchains. While private blockchains maintain the immutability of transactions, they may restrict the visibility of data and transactions to authorized participants. The level of transparency can be adjusted based on the network's requirements. Private blockchains can achieve higher transaction speeds and scalability compared to public blockchains since they have a limited number of participants and can use more efficient consensus algorithms.

2.3 Blockchain Platforms

2.3.1 Bitcoin

Bitcoin is the pioneering blockchain platform that introduced the concept of decentralized digital currency. It operates on a public blockchain, utilizing the Proof of Work (PoW) consensus algorithm. Bitcoin's primary focus is on enabling peer-to-peer electronic cash transactions, aiming to provide a secure and censorship-resistant alternative to traditional financial systems. It has a limited scripting language that allows for programmability to a certain extent. Bitcoin's native cryptocurrency, BTC, is widely recognized and serves as a store of value and medium of exchange.

2.3.2 Ethereum

Ethereum is a programmable blockchain platform that extends beyond digital currency, enabling the development of decentralized applications (DApps) and smart contracts. It introduced the concept of a Turing-complete scripting language, which allows

developers to build and deploy a wide range of decentralized applications on its public blockchain. Ethereum employs the PoW consensus algorithm, but it is transitioning to a more energy-efficient PoS consensus mechanism called Ethereum 2.0. Ethereum's native cryptocurrency, Ether (ETH), is used as both a fuel for executing transactions and a means of fundraising through Initial Coin Offerings (ICOs) and Decentralized Finance (DeFi) applications.

2.3.3 Hyperledger

Hyperledger is not a single blockchain platform but rather a collection of open-source blockchain frameworks and tools developed by the Linux Foundation. It focuses on providing enterprise-grade blockchain solutions for various industries. Unlike Bitcoin and Ethereum, Hyperledger frameworks, such as Fabric and Sawtooth, are permissioned blockchains, offering increased privacy, scalability, and governance control. Hyperledger frameworks allow organizations to collaborate, share data, and streamline business processes securely. They support modular architecture, pluggable consensus algorithms, and flexible smart contract execution engines, making them suitable for enterprise use cases like supply chain management, healthcare, finance, and more.

Blockchain Characteristics Comparison			
Characteristics	Bitcoin	Ethereum	Hyperledger
Permission restrictions	Permissionless	Permissionless	Permissioned
Restricted public access to data	Public	Public or private	Private
Consensus	Proof of work	Proof of work	PBFT
Scalability	High node-scalability, Low performance-scalability	High node-scalability, Low performance-scalability	Low node-scalability, High performance-scalability
Centralized regulation	Low, decentralized decision making by community/miners	Medium, core developer group, but EIP process	Low, open-governance model based in Linux model
Anonymity	Pseudonymity, no encryption of transaction data	Pseudonymity, no encryption of transaction data	Pseudonymity, encryption of transaction data
Native currency	Yes, bitcoin, high value	Yes, ether	No

CHAPTER 3
CHALLENGES IN CURRENT HEALTHCARE SYSTEM

The healthcare system faces several data challenges that impact patient care, research, and operational efficiency. These challenges arise due to the complex nature of healthcare data and the various stakeholders involved. Here is a detailed explanation of some key data challenges in the healthcare system:

3.1 Data Fragmentation

Healthcare data is often scattered across multiple systems, such as electronic health records (EHRs), imaging systems, lab systems, and specialized databases. These systems may not be interoperable, meaning they cannot easily exchange or access data with each other. As a result, patient information is fragmented and not readily available to all relevant healthcare providers. This fragmentation hampers care coordination, increases the risk of medical errors, and limits the ability to gain a holistic view of a patient's health history. Efforts to promote interoperability standards, such as Fast Healthcare Interoperability Resources (FHIR), aim to address this challenge by facilitating the seamless exchange of healthcare data.

3.2 Data Silos and Lack of Interoperability

Data silos occur when different healthcare organizations or departments within the same organization use separate systems that do not communicate effectively. For example, a hospital may have its own EHR system, while outpatient clinics use different EHR systems. This lack of interoperability leads to challenges in sharing patient data, resulting in redundant data entry, delays in accessing information, and potential errors. Standardization of data formats and the adoption of common data exchange protocols are crucial to break down these silos and enable seamless data sharing.

3.3 Data Security and Privacy

The healthcare industry faces significant challenges in ensuring the security and privacy of patient data. Cyberattacks, data breaches, and ransomware incidents continue to threaten healthcare organizations, compromising patient confidentiality and trust. The sensitive nature of healthcare data, which includes personal health information (PHI), makes it highly valuable to attackers. Healthcare organizations need to invest in robust cybersecurity measures, such as firewalls, encryption, intrusion detection systems, and employee training on best practices. Compliance with regulations, such as HIPAA in the United States, is crucial to safeguard patient data and avoid legal consequences.

3.4 Data Quality and Accuracy

Data quality is paramount in healthcare to ensure accurate diagnoses, appropriate treatments, and patient safety. However, data inconsistencies, errors, and missing or outdated information can lead to medical errors and compromised care. Data quality issues may arise due to manual data entry, variations in data capture practices, or limited validation mechanisms. Implementing standardized data capture templates, automated data entry systems, and data validation processes can help improve data quality. Regular data auditing and monitoring are also important to identify and rectify inaccuracies promptly.

3.5 Data Governance and Management

Establishing effective data governance frameworks is essential for managing healthcare data efficiently and ensuring its integrity, accessibility, and long-term retention. Data governance involves defining roles, responsibilities, and processes related to data management, including data ownership, stewardship, and consent policies. Organizations need to establish data governance committees, develop data management policies, and ensure compliance with regulatory requirements. This includes defining data retention periods, establishing data backup and recovery mechanisms, and ensuring appropriate access controls to protect sensitive information.

3.6 Data Analytics and Insights

The healthcare system generates vast amounts of data that can provide valuable insights for clinical research, population health management, and decision support systems. However, extracting meaningful insights from this data can be challenging. Data analytics initiatives face hurdles such as data standardization, data cleansing (removing errors and inconsistencies), and ensuring patient privacy while enabling research. Advanced analytics tools, including machine learning and artificial intelligence, can assist in analyzing large datasets and extracting actionable insights. Healthcare organizations need skilled data analysts, robust infrastructure, and secure data sharing platforms to leverage the potential of data analytics effectively.

Addressing these data challenges requires innovative solutions and technologies. Blockchain, as discussed earlier, can contribute to mitigating several of these challenges by providing secure, interoperable, and auditable data management capabilities. However, it's crucial to consider a holistic approach, including data governance, standardized data capture, robust cybersecurity measures, and efficient data integration and analytics, to fully address the data challenges in the healthcare system.

CHAPTER 4
BLOCKCHAIN APPLICATIONS IN HEALTHCARE

Blockchain technology has the potential to transform the healthcare industry by addressing various challenges related to data security, interoperability, privacy, and efficiency. Blockchain can facilitate secure and standardized sharing of patient health records and other medical data across different healthcare providers and systems. By creating a decentralized and immutable ledger, blockchain enables patients to have greater control over their data and easily share it with authorized healthcare providers when needed, leading to improved care coordination and continuity. The decentralized nature of blockchain, combined with cryptographic algorithms, enhances data security by protecting sensitive health information from unauthorized access or tampering. There are multiple factors which motivated researchers to move towards usage of blockchain in healthcare because of the improvement that it brings into the current system, some of the

4.1 Security and Privacy

As blockchain is a decentralized system, it ensures no single point failure which could be faced in the current data management system where all the medical data is kept at a single centralized server. All the data on the blockchain is encrypted to make it secure from cyber attacks, blockchain uses the concept of public and private key therefore a person with the correct private key can only access the data.

One of the principles for which blockchain is widely adopted is consensus algorithm. Consensus algorithm refers to agreement of the nodes in the network before making any modification to any node or adding a new node to the chain. Therefore to make any false changes to the chain, the attacker must have control 50% of the network which is almost impossible.

Having no way to falsely modify the blocks or the medical records could be helpful in the healthcare system. This property can benefit to reduce medicare frauds which generally happen due to middle person involvement.

4.2 Real time data access

Motivation behind moving towards blockchain and giving up the traditional method of storing medical records is that it's hard for patients to have a complete history of their treatment if they have referred multiple care delivery organizations.

Blockchain aims to keep a dedicated track with proper timestamp of treatment a patient has received from different healthcare centers.

Blockchain allow patients to access their entire medical history which they might have recieved from different healthcare center at one point. Having a detailed report of the treatment allows holistic views of patients, personalized medical treatments, and efficient communication between patient and doctors.

Updation done by a healthcare center about a patient's treatment can be accessed by the patient from any point. Blockchain will maintain a decentralized copy of the patient's report for it to be retrieved at realtime from the desired system.

4.3 Improved Transparency

One of the principles which lead to consideration of blockchain for the healthcare sector is that any changes made to the blockchain will be visible to all the participants of the network. Its use case in healthcare is that if any unauthorized entity tries to change the data it can be diagnosed. Transparency of data in healthcare can be used in multiple ways like tracking of pharmaceutical raw material to finished goods, and tracking drug supply chains. Having such a transparent system allows for multiple participants and jurisdiction. In the current system documents can be faked as there is a central authority which can be compromised. Thus transparency can bring down the rate of medical fraud.

4.4 Exclusion of Third party involvement

Medical industry is facing many issues and losses because of the involvement of third parties or mediators. Removal of third parties could be beneficial in many ways like drug supply, medical insurance claim. Drug supplies involve many illegal activities in the current system, one of main issues of concern is counterfeit drugs. With the current system drugs supply chain is insufficient it involves interference of many parties. Thus as an improvement to this could be an introduction of blockchain in the supply chain. Decentralized, digital ledger helps to keep a track of movement of the medicines.

4.5 Anonymity

Real Time medical data of patients is used by researchers to have correctness and accuracy in their work. But at the same time it is necessary to maintain the anonymity of patients whose data is considered for the research. In blockchain nodes contain sender and receiver names in encrypted form. Through blockchain one can help medical experts with his real time medical data without reliving his identity in any manner.

CHAPTER 5
PROPOSED MODEL TO MANAGE DATA STORAGE

5.1 Abstract

To overcome the drawbacks of centralized system to store medical records a decentralized app or DApp is designed. It will allow us to implement the concepts of blockchain to maintain the patient records in a decentralized manner. Application reflects the benefits of using blockchain over current healthcare systems like immutability, security and efficient sharing of data between two trusted parties. It is designed around the actual scenarios used in medical fields to communicate data between patient and doctors. The application consist of 2 actors patient and doctor. Patient can register to the application by providing his etherum address. Once registered he can provide his

5.2 Software Requirements

5.2.1 Ganache

Ganache is a software tool developers use to create a local blockchain network for testing and development purposes. Developers may effectively test and troubleshoot their blockchain apps by simulating a blockchain network on their local PC with Ganache. Ganache supports the quick development of distributed applications using Ethereum. Two versions of Ganache are available: a user interface (UI) and a command line interface (CLI). With Ganache UI, developers can quickly communicate with the local blockchain. In addition to offering real-time data on accounts, balances, transactions and events, it also has tools for testing and debugging smart contracts.

5.2.2 Truffle

Truffle provides a development environment for blockchain. It facilitates the developer with testing framework for blockchain applications. It has configured features for

deployment, integration and compilation. The features of network management in the Truffle development framework can help us deploy applications to any number of public and private networks.

5.2.3 MetaMask

MetaMask is an extension which can be added to brower to access Ethereum enabled distributed applications or “Dapps”. MetaMask injects the API ot ethereum web3 into javascript context of website, so that dapps the user is working on can read from the blockchain. It is one of the most popular wallet for cryptocurrency and it supports a large variety of Ethereum based tokens and NFTs.

5.3 System Features

- The registration process is kept simple for the application. The patient only needs to enter his ethereum address or the private key to take part in the transactions.
- Once registered patient can navigate to “give permission” page to create a permission by entering his ethereum address and the respective doctors’s ethereum address.
- Giving permission allow doctor to create new records against the patients address. If the permission is not given by the patient then a doctor cannot a create random records while are later added to the patients medical history. This feature allow patient to maintain integrity of his medical records.
- "Create record" section allows the doctor to write a prescription by entering his and the respective patient's details. The doctor needs to enter his private key to sign the medical record so that the authenticity of the record can be checked later. Along with the doctor ethereum address, the patient's private key is also entered to map it to an appropriate patient.
- Once the record is created by default, patients and doctors are allowed to view the record.

- The stakeholders can view the record by accessing the "view" section and by entering the private key of the person who wants to view the record and record name. If the respective person is a doctor or the patient to whom the record belongs then the record will be displayed otherwise an error will be shown. Thus maintaining the confidentiality of the data.
- But the medical record can also be shared to any node in the network by giving permission through their private key.
- Through the "share" section the patient can allow other nodes or participants on the network to access the record by entering their ethereum address and the record name which need to be shared.
- Allowing other participants on the network to view and validate data, which one of the main requirement in healthcare system that is exchange of medical records as it can helpful in research and other aspects of the industry.

CHAPTER 6
LIMITAIONS OF BLOCKCHAIN IN HEALTCARE

6.1 Scalability

When it comes to sectors like healthcare data is generated at huge amounts every minute from every part of the world. Handling large data requires an efficient system which is getting hard for our current setup in healthcare. Blockchain was initially developed to fulfill the requirements of the financial world, in financial transactions data are very small in size and only stores transaction details whereas in the healthcare sector data to be stored in blocks are large in size. As the load of data increases on the server, transaction speed also is affected.

6.2 Interoperability

Within the advancement in technology the healthcare system is equipped with many different devices, technologies and components. Using blockchain in healthcare definitely has many benefits but the use of blockchain in actual sense means making it compatible with the existing healthcare system. To adapt blockchain in the healthcare system, we require to integrate all the modern technologies and devices with blockchain but due to reasons like interoperability integration gets complex. To get best out of blockchain it's important to form an ecosystem where even data generated from patient centric devices like wearables are also kept in the loop, such data are currently ignored when maintaining a patient's medical data.

6.3 Transferring of existing data

Current healthcare system has come a long way and is well developed to handle today's health sector. Data on existing systems is not organized or follows standards that an ideal system should, but that's because the current system is a compilation of years of slow development. When we plan to switch to a new technology it is important to consider transfer of data to a new platform.

6.4 Lack of technical skills

Blockchain being a new technology in the market its future depends upon the developers community. When a new technology is picked up by developers it tends to go in different directions but on conditions that it suits the developers, easy to understand for them, helps to solve their problem statements in a more efficient way then existing technology. Therefore at initial level huge efforts need to be made by the current existing small community of blockchain developers.

6.5 High energy consumption and slow processing speed

Blockchain gained popularity because of one its principle, the consensus algorithm. But as consensus uses proof of concept, the process consumes a lot of computing power for the miners to solve the hash to add a block to the network. There are different approaches to reach consensus like rather than using proof of concept one can use proof of stack but it also has its risks. Throughput of blockchain can be compared by taking an example from the financial world, throughput given by blockchain is around 7 transactions per second whereas mainstream payment processing techniques are compared like visa it gives an output of 24000 transactions per second.

CHAPTER 7
FUTURE DIRECTIONS AND RESEARCH OPPORTUNITIES

7. 1 LightWeight Blockchain

Researchers recently started to see the potential of adapting blockchain in healthcare. In the last three to four years many proposals have been made for different types of blockchain network that could be used in the healthcare sector but most of the approach is inspired from the financial field where the bitcoin network is one of the trusted networks. But healthcare sector and financial sector cannot be compared and it is not efficient to adapt same practices of financial world in health sector, reason to support this statement is that in financial world data to be stored are small in size, they only contain information about the transaction, whereas when healthcare sector is considered electronic health records are more detailed and data contained.

Some of the recent work suggests use of bitcoin network in healthcare but bitcoin network suffers from many drawbacks like scalability issue, it has low transaction throughput and high energy consumption.

To overcome the challenges of the traditional bitcoin network a lightweight blockchain has been proposed by researchers. Light weight blockchain focuses on reducing computation and communication burden as compared to the traditional blockchain network. High computational overhead was one of the factors to reconsider using the initial bitcoin network. Researchers could achieve to lower both the things by dividing the network nodes into clusters. Each cluster maintains a copy of the ledger rather than each node that we see in the bitcoin network. The proposed model architecture doesn’t fork the transaction on all the participant nodes like we do in the bitcoin network, only the clusters that we have created will have one cluster head that will maintain a copy of the ledger.

7.2 Handling future pandemics more efficiently

Humans can never be sure about upcoming pandemics like we saw covid-19 which affected the whole world, we can just be prepared enough to handle such conditions in a more efficient manner. With the current healthcare system, where data sharing is less efficient, data is less secure, it was hard for researchers to have full knowledge about the ongoing condition. If technology like blockchain is introduced in the healthcare sector, it becomes easy for research to access data. Currently everything is distributed on disconnect systems. This presence of data on different systems makes it a tedious job to collect and compile all the information.

7.3 Creation of new Token

Introduction of blockchain in any field comes with creation of a digital asset. Cryptocurrency and blockchain work hand in hand, cryptocurrency act as incentive for the work done in maintaining the blockchain. As blockchain will be used to maintain health records the nodes which are contributing towards the handling of data will be rewarded with a token. With the increasing acceptance of cryptocurrencies in the market, this new crypto could attract more miners towards the development of the technology in the medical field.

7.4 Insurance Claims

Medical fraud is one of the major issues that authority has to deal with. In the USA a fraud of $30 million was reported in 2016. Blockchain being a digital ledger where data remains immutable makes it difficult for fraudsters, transactions can only be accessed by authorized nodes in the network. Smart contacts of blockchain can be used to automate the process of validating claims and thus improving customer service.

7.5 Training and Education of Medical Professionals

With the regular advancement in the medical field, it's important for medical learners to cope up with the rapid evolution. As we know digital platforms have become a more common source for learning, it's important to know the authenticity of the data selected for learning. On the internet it is not easy to trace and verify the source of medical content that is being shared.

Therefore, a scope to use blockchain as a healthcare education platform exists, with the traceability that blockchain provides learners can be sure about the resource that is reaching them.

7.6 Improved Data Auditing

Healthcare being an intense field where small negligence could lead to risking someone's life. Therefore it's important to keep a check whether care delivery organizations are following all the regulations and standards set by higher authorities. Currently the healthcare systems are manual which makes it difficult to audit the records and activities, being a manual approach there is no smart direction towards the process.

CHAPTER 8
CONCLUSION

In the last 3 years the healthcare sector has been a point of attention due to covid-19 pandemic. It was crucial to see how the current healthcare system manages sudden increase in data due to this pandemic. With such a situation being faced it is now important to attend all the drawbacks that were seen with the current system. Inefficiency in the present system which slowed our fight towards covid or any pandemic that would have come were privacy, security, management and sharing of data. It's important to extend our reach to explore new technologies to handle our healthcare sector. One of the booming technologies which is being adapted in multiple sectors recently is blockchain. Blockchain being based on principles of cryptography, decentralization and conceus makes it ideal for industry where privacy and security of data is crucial and efficient data sharing gives blockchain an edge towards considering it for the healthcare field.

Each technology has its strengths and weaknesses similarly blockchain being a new technology in the market comes with few drawbacks. But as blockchain is being adopted in multiple sectors its strengths somehow outweighs its weak points. This thesis has explored the application of blockchain technology in the healthcare system to address data security, privacy, and interoperability challenges. Through an in-depth analysis of the existing data challenges in healthcare, the need for a robust and secure infrastructure has been established. Blockchain technology, with its decentralized and immutable nature, offers promising solutions to overcome these challenges and revolutionize the healthcare industry. While blockchain technology shows great promise, the thesis acknowledges its limitations, such as scalability challenges and the need for standardization. Future research should focus on addressing these limitations and exploring potential solutions to ensure the scalability and widespread adoption of blockchain in healthcare.

In conclusion, this thesis contributes to the growing body of knowledge on blockchain technology in healthcare. It provides valuable insights for healthcare practitioners,

policymakers, and researchers, highlighting the potential of blockchain to transform the healthcare system by enhancing data security, privacy, and interoperability. By leveraging blockchain, healthcare can become more efficient, patient-centric, and resilient in the face of evolving data challenges.

REFERENCES

1. Katuwal, Gajendra J., et al. "Applications of blockchain in healthcare: current landscape & challenges." arXiv preprint arXiv:1812.02776 (2018).

2. A. A. Mazlan, S. Mohd Daud, S. Mohd Sam, H. Abas, S. Z. Abdul Rasid and M. F. Yusof, "Scalability Challenges in Healthcare Blockchain System—A Systematic Review," in IEEE Access, vol. 8, pp. 23663-23673, 2020, doi: 10.1109/ACCESS.2020.2969230.

3. L. Ismail, H. Materwala and S. Zeadally, "Lightweight Blockchain for Healthcare," in IEEE Access, vol. 7, pp. 149935-149951, 2019, doi: 10.1109/ACCESS.2019.2947613.

4. Bazel, Mahmood & Mohammed, Father & Ahmad, Mazida. (2021). Blockchain Technology in Healthcare Big Data Management: Benefits, Applications and Challenges. 1-8. 10.1109/eSmarTA52612.2021.9515747.

5. L. Soltanisehat, R. Alizadeh, H. Hao and K. R. Choo, "Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review," in IEEE Transactions on Engineering Management, doi: 10.1109/TEM.2020.3013507.

6. R. Zhang, R. Xue and L. Liu, "Security and Privacy for Healthcare Blockchains," in IEEE Transactions on Services Computing, doi: 10.1109/TSC.2021.3085913.

7. Niranjanamurthy, M., Nithya, B.N. & Jagannatha, S. Analysis of Blockchain technology: pros, cons and SWOT. Cluster Comput 22, 14743–14757 (2019). https://doi.org/10.1007/s10586-018-2387-5

8. M. Kassab, J. DeFranco, T. Malas, P. Laplante, G. Destefanis and V. V. G. Neto, "Exploring Research in Blockchain for Healthcare and a Roadmap for the Future," in

IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 4, pp. 1835-1852, 1 Oct.-Dec. 2021, doi: 10.1109/TETC.2019.2936881.

9. Tseng, J.-H.; Liao, Y.-C.; Chong, B.; Liao, S.-w. Governance on the Drug Supply Chain via Gcoin Blockchain. Int. J. Environ. Res. Public Health 2018, 15, 1055. https://doi.org/10.3390/ijerph15061055

10. Mohsen Attaran (2020): Blockchain technology in healthcare: Challenges and opportunities, International Journal of Healthcare Management, DOI: 10.1080/20479700.2020.1843887

11. Ekblaw, Ariel, et al. "A Case Study for Blockchain in Healthcare:“MedRec” prototype for electronic health records and medical research data." Proceedings of IEEE open & big data conference. Vol. 13. 2016.

12. Onik, Md Mehedi Hassan, et al. "Blockchain in healthcare: Challenges and solutions." Big data analytics for intelligent healthcare management. Academic Press, 2019. 197-226.

13. Bell, Liam & Buchanan, William & Cameron, Jonathan & Lo, Owen. (2018). Applications of Blockchain Within Healthcare. Blockchain in Healthcare Today. 10.30953/bhty.v1.8.