Using Smart and Secret Sharing for Enhanced Authorized Access to Medical Data in Blockchain

by

Abdihakim Mao

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of

Master of Information Technology

in

Digital Media

Carleton University
Ottawa, Ontario

© 2020, Abdihakim Mao

Abstract

In this thesis, we analyze the challenges of using and sharing electronic health information exchange (HIE) in hospitals and clinics. In Canada, there is a lack of HIE platforms that provide interoperability for hospitals and other medical institutions across the country. In this research, we explore a potential use case of utilizing blockchain technology as a tool to facilitate better HIE between users involving patients, doctors, and researchers. Our proposed proof-of-concept evaluates the impact of implementing smart contracts to assist in automating the digital identity and access management of medical data via the use of public-key cryptography. In addition, we apply Shamir's secret sharing scheme by distributing the public keys to safeguard better the identities and data of users in our system. We evaluate our proposed solution in the context of scalability, complexity, and efficiency, as well as comparing our approach to other blockchain-based healthcare solutions.

Acknowledgments

All praise is due to Allah, the Most Gracious and the Most Merciful. I want to begin by thanking God for all the opportunities, obstacles, strength, blessings, and for allowing me to finish my thesis. Being able to study in a post-secondary institution has been a long and challenging process for me.

I begin by thanking my family, in particular, my parents, who played a big part in not giving up on me and supporting me to get my master's degree and to seek post-secondary education. To my siblings, thank you for your experiences, support, and encouragement.

I wish to express my deepest gratitude to my supervisor, Prof. M. Omair Shafiq. Without his knowledge, guidance, patience, perseverance, belief, kindness, and ability to listen, I could not have completed my thesis. I am indebted to him for the continuous support, encouragement, and leadership, and for that, I will be forever grateful.

I want to pay my special regards to the fantastic staff of professors at the School of Information Technology. Thanks to Dr. Ali Arya, Dr. Chris Joslin, and Dr. Audrey Girouard for providing their expertise and experiences. I also wish to show my gratitude to the exceptional administrative staff. Thank you, Ms. Erenia Oliver, Ms. Ria Akaiwa, and Ms. Hana Jabi for providing their vital support and assistance every step of the way.

I wish to show my gratitude to my friends that I have met along my journey of completing this thesis. To Diego Zambrano, I thank you for all the support and advice. Secondly, to Matt Ma, thank you for your knowledge of programming and understanding. To all my friends and classmates, I thank you for your friendship.

Last but not least, thank you to Carleton University for allowing me to learn and grow as a person. Attending Carleton University was life-changing. I will always remember and cherish the two years I have spent here.

Once again, I thank Allah, my sustainer, for making all this possible, and all praise goes to him.

Table of Contents

List of Tables

List of Figures

List of Appendices

Chapter 1: Introduction

In today's technological age, vast amounts of information regarding modern healthcare practices have become easily accessible via the internet. With the widespread use of information and technology tools such as computers, smartphones, and tablets, individuals can monitor their health without physically visiting a medical doctor. In some cases, visiting a medical doctor can be a cause of financial burden for individuals unable to afford proper healthcare. On the other hand, individuals who have access to good healthcare in most cases experience long wait times before seeing a medical doctor.

Nowadays, the emergence of electronic health (e-health) services is becoming a popular trend for individuals to get immediate attention surrounding health-related diagnoses without visiting a hospital. The term e-health covers a broad area encompassing the electronic processes and communication of traditional healthcare practices. As mentioned in the Journal of Medical Internet Research describes e-Health as the intersection of medical informatics, public health and business enhanced through the internet and related technologies [1]. Additionally, governments also have their definition regarding the term of e-health. For instance, the Government of Canada defines e-health as the application of information and communications technologies in the health sector surrounding administrative duties such as electronic patient administration systems and covering health care delivery [2]. E-health is also the use of computer systems and smart devices by nurse practitioners and pharmacists for patient management. Lastly, the World Health Organization (WHO) explains that e-health is the cost-effective and secure use of information and communications technologies supporting health-related care, surveillance, literature, education, and research [3]. Examples of services that recognize as e-health

because of their digital presence include electronic health records, virtual healthcare, and mobile healthcare.

In today's digital age, access to health knowledge is more accessible with the use of online healthcare publishers. Currently, there are vast amounts of health information available online about symptoms for certain diseases, medication side effects, and treatment practices. As reported by the medical library association, the top health websites include the Centers for Disease Control and Prevention (CDC), healthfinder® and Kidshealth® [4]. As a result of health resources being widely available, individuals can seek self-treatment from medical websites and health discussion forums. However, despite the presence or consultation of a doctor, the quality of healthcare data found online can be less detailed and inaccurate at times. According to a study in 2016 about the Comparison of Physician and Computer Diagnostic Accuracy published by The Journal of the American Medical Association, physicians vastly outperformed computer algorithms in diagnostic accuracy (84.3% vs. 51.2% correct diagnosis according to the top 3 diagnoses listed). Consequently, individuals using online websites for diagnosis purposes are not obtaining higher accuracy information as oppose to when visiting a doctor.

Patients and health-care professionals communicate based on established common values of responsibility, accountability, and trust. With patients often relying on doctors for their expert advice on health-related issues, there can be many factors and barriers that can surface, which prevents patients from visiting a health practitioner. According to a study published by the National Center for Biotechnology Information (NCBI), reasons for avoiding medical care include receiving unfavourable evaluations (33% of 1,369 participants of the study), high cost (24%), time constraints (15.6%) and no health

insurance (8.3%) [5]. Subsequently, analyzing the obstacles limiting patient access to health providers will assist in developing better strategies and recommendations for removing barriers to access to healthcare.

In the field of e-health or digital health, many terms describe health records that are shared and accessed digitally. According to Canada Health Infoway, there are three generally used terms to describe digital health records [6]. These terms are electronic medical records (EMR), electronic health records (EHR), and personal health record (PHR). To better explain these terms in detail, Table 1 describes the differences in each of these terms. EMR and EHR are terms that are commonly indistinguishable and used interchangeably.

Digital Health Records	Completeness of Records	Provider of Records	Examples
• EMR – Electronic Medical Records	• Partial health records	• Health Care Provider	• Data used to provide diagnosis and treatment to a patient [7]
• EHR – Electronic Health Records	• Complete health records	• Health Care Provider	• Patient demographics, medical history, allergies, lab results, and billing information [7]
• PHR – Personal Health Records	• Partial or Complete health records	• Patient	• Patient demographics, medical history, allergies, lab results, and billing information [7]

Table 1 Description of Various Digital Health Records

1.1 Background

In this thesis paper, our primary objective is to improve the accessibility of EMR's of patients focusing on using blockchain technology. With the emergence of blockchain technology, patients' medical information can be easily authenticated and processed more accurately. Blockchain is a publicly accessible digital ledger that records transactions

chronologically with shared business processes [8]. The primary purpose of the use of blockchain technology is to reduce the cost of trust between two parties. In the context of the financial industry, centralized local establishments such as banks are relied on to validate money transactions between clients. For example, once Client A sends money to Client B, the bank must verify Client A has money in their account. In this example, the bank represents the intermediary between Client A and Client B by recording the interactions between clients in a localized database. Therefore, relying on a central local server can be regarded as inefficient, given its limited amount of trust.

Due to the widespread use of Bitcoin, which is a form of electronic currency, has increased the market value of blockchain technology. Currently, bitcoin uses blockchain technology to verify and regulate the transfer of funds between individuals. Blockchain technology uses a secure way to identify and authenticate sensitive data. Additionally, blockchain reduces the time of validating transactions by removing the dependency of a centralized third party. Conventionally, money transfers made through intermediaries such as banks and credit unions often result in several downsides, including high fees as well as extra time is required to transfer money. Seeing as blockchain's digital ledger is publicly accessible, users can validate and add transactions to the ledger faster and cheaper.

Accordingly, distributed technologies such as blockchain have reduced the cost of trust by sharing the costs among multiple trusted associates. Therefore, transactions stored in a blockchain are distributed across different servers, thus decreasing the cost of trust. Given the use of Bitcoin, users can earn a small incentive for validating a transaction, which, as a result, ensures the security and accuracy of the ledger. Overall, blockchain technology attempts to remove costs and reduce risks among users.

Moreover, blockchain aims to improve business processes that involve digital supply chains. Many issues concerning digital health records are stemming from a shortage of information sharing and a lack of coordination among healthcare professionals. As a result, digital supply chain systems found in hospitals are not utilizing their full potential — another area where blockchain can improve an organization's information strategy involves big data analytics. With increased complexities and opportunities for information sharing in the healthcare sector, distinguishing which data is the most accurate can be difficult. Therefore, blockchain can consistently validate the information based on an established set of protocols.

Furthermore, the four main capabilities encompassing a blockchain are transparency, disintermediation, auditability, and transfer of value. Each of these capabilities represents a requirement for building a blockchain system. Firstly, transparency implies that all added blocks of information are linked in a chain. Using a chain-like system improves the integrity of information by following a single sequence approach. Secondly, disintermediation refers to the role of distributed intermediaries that enable trust and transparency in a blockchain. Thirdly, auditability refers to the data stored on the blockchain that is immutable and cannot be altered or deleted. In turn, blockchain provides a lower cost alternation for record-keeping. Lastly, transfer of value refers to the process of blockchain exchanging information faster, safer and for less cost. Blockchain use of cryptography allows for information to be transferred or exchanged at a low cost with a similar or a higher level of trust [9].

1.2 Structure of Blockchain

Blockchain technology is a combination of various technologies put together. Firstly, blockchain uses public and private key encryption through the use of cryptography that secures data transmission, storage and user authentication [10]. Cryptography prevents data from being stolen, corrupted, modified or deleted on the blockchain. As a result, blockchain uses public and private key cryptography to decrypt and encrypt transactions. A public key and a private key are similar to a piece of login information, wherein the public key is the username, and the private key is the password. Thus, public keys can be shared quickly, allowing users to send encrypted messages and verify digital signatures.

In contrast, private keys are kept hidden, allowing users to receive decrypted messages and create digital signatures [11]. Under blockchain, cryptography is also in the application of digital signatures. Hence, a digital signature provides approval of a transaction sent in the blockchain by using an individual's private key [11]. Therefore, once the recipient receives the data, the recipient's data is then decoded through the decryption of the private key. To send or receive a message on the blockchain, possession of both the public and private keys are needed.

Another technology used by blockchain includes a peer to peer model of communication. In the peer to peer (P2P) distributed network, each node acts as a peer by storing and sharing messages sent in the blockchain. Thus, each node in the blockchain network can store a digital copy of all the transactions sent in the blockchain. Functionalities of the P2P network include uploading and downloading data from other nodes in the network, querying nodes to find and download data, and sourcing uploaded or downloaded data for other nodes in the network [12].

Features	Public Blockchain	Private Blockchain	Hybrid Blockchain
• Permissions	• Unrestricted Access	• Restricted Access	• Partial Restricted Access
• Consensus Mechanism	• Performed by all Nodes	• Performed by a Single Node	• Performed by Selected Nodes
• Speed (Transactions Per Second) [14]	• Low • (Bitcoin 7 transactions/second)	• High • (Ripple 1500 transactions/per second)	• High • (Hyperledger 3000 transactions/per second)
• Scalability	• Low	• High	• High
• Centralization	• Low	• High	• Medium
• Transparency	• High	• Medium	• Medium
• Examples [15]	• Bitcoin, and Ethereum,	• Ripple (XRP), and Corda	• Hyperledger, and Dragonchain

Table 2 Types of Blockchain Platforms

Moreover, blockchain technology is a secure platform that reduces the cost of trust among users. Presently, the three main types of blockchain platforms that exist include a public blockchain, a private blockchain and a hybrid blockchain [13]. According to table 2, each type of blockchain has distinctive features, advantages and disadvantages.

Firstly, a public blockchain is a distributed permission-less ledger system that allows anyone to access and verify transactions. The advantages of a public blockchain include high-security protocols given the use of nodes mining and approving transactions. Another advantage of a public blockchain is its high transparency as transactions performed are visible to all users in the network. A disadvantage of a public blockchain includes the low processing speed of verifying transactions and high energy consumption when nodes are mining blocks.

Secondly, a private blockchain is a permissioned system that restricts nodes or users to access and store transactions in the network. Thus, each user in the blockchain must be pre-identified. The main advantages of a private blockchain system include faster

processing of transactions and better scalability. A drawback of private blockchain includes having a small number of users. As a result, there is a higher security risk for data on the blockchain to be hacked or misused.

Lastly, a hybrid blockchain is a combination of both the public and private blockchain systems. Therefore, a hybrid blockchain is a flexible system as users can be part of the network. On the other hand, users can control the accessibility of transactions stored on the blockchain. Another feature of hybrid blockchains involves users who can choose whether to verify transactions based on the central authority of the network or by other nodes in the network. An advantage of a hybrid blockchain system is the higher processing of transactions per second. A disadvantage of a hybrid blockchain system includes its centralization of nodes, which in turn can reduce the functionality and purpose of using a blockchain-based system.

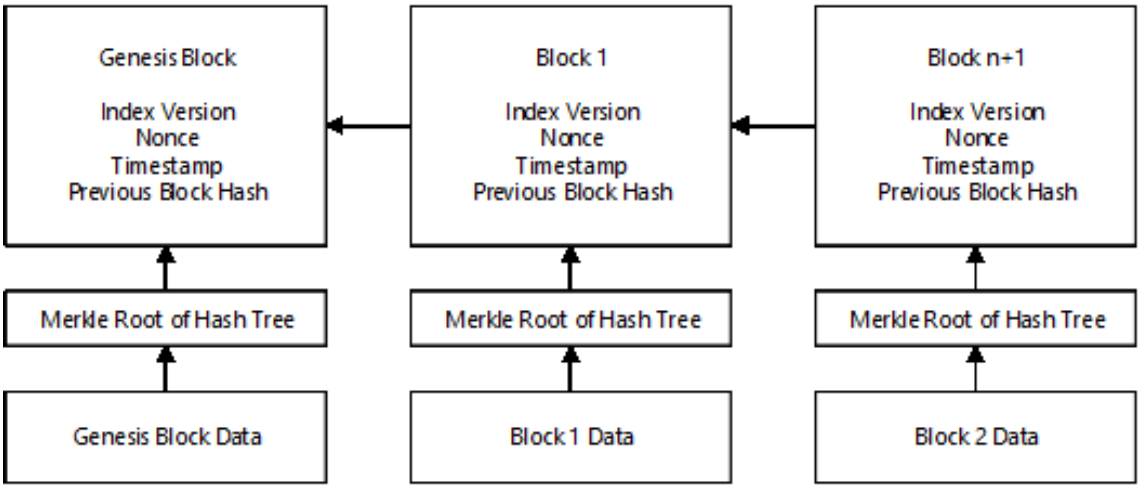


Figure 1 Structure of Blocks

Furthermore, blockchain uses blocks as folders to store transactions. As shown in figure 1, each block must follow a specific format for recording transactions. The first block created in a blockchain is called the genesis block. In the genesis block or referred to as block 0, is the starting point in which all blocks created in a blockchain are traceable.

Each block contains information including the block number, the timestamp, the nonce value, the previous hash function, and the root hash of the Merkle tree.

1.3 Smart Contracts in Blockchain

In the context of blockchain, a smart contract is an application or protocol that verify terms of a contract via computer code [16]. Smart contracts are transforming traditional contracts by enforcing statements in the contract without the need for a third party. With the risk of traditional contracts not fulfilling some elements of a contract, a smart contract can check and enforce the fulfillment of every condition in the contract. Seeing as smart contracts are secure as a result of being based on cryptography, contracts can be distributed and verified across many trusted nodes in the network.

With cryptocurrencies being the most popular use case of blockchain technology, Bitcoin is the first blockchain platform to use smart contracts to execute codes in the network. However, it is essential to mention that smart contracts became popular with the creation of the Ethereum protocol [16]. The main advantages of using a smart contract include its ability to be customizable. Thus, having a smart contract model can offer a solution or service to a specific problem. The disadvantage of using a smart contract contains risks as the computer code used to write the smart contract may contain bugs or loopholes.

1.4 Blockchain and E-Health in Canada

The Canadian Healthcare System is famously known for providing universal free healthcare to all Canadians residing in Canada. Large amounts of healthcare information are mostly available in computers at hospitals. Seeing as most of the healthcare information is used for providing patients with hospital services and informing the government. Health

records are currently not being utilized fully due to the lack of integrated electronic systems providing a network for sharing data. There are many opportunities in establishing an e-Health network for patients, healthcare institutions and the government. Nowadays, many medical professionals are using electronic tools to provide better care services to patients. In Figure 2, the Canadian Medical Association Physician Workforce Survey 2017 reports that 82% of physicians access lab tests and diagnostic results using electronic tools; additionally, 66% of physicians access a list of medications taken by a patient electronically [17]. Correspondingly, the use of digital health tools such as patient portals and virtual visits can make health information and services accessible electronically. However, with there being little to no networks that provide an integrated and enhanced information sharing system, there is less transparency for patients to manage their health data electronically. Therefore, with overhead costs representing a significant component of hospital expenditures, hospitals are investigating in cost-cutting opportunities in order to reduce costs associated with data redundancy, communicating with patients regarding lab results by telephone, and providing timely access to health information [18].

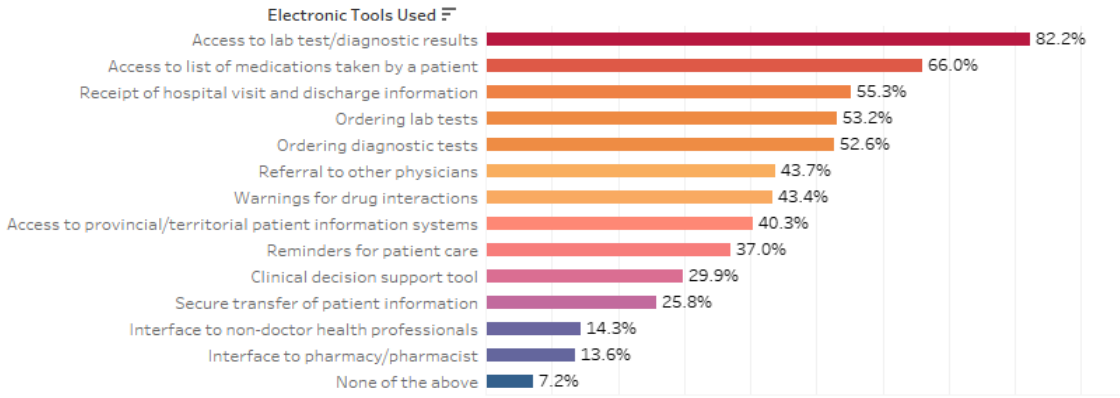


Figure 2 Electronic tools used by Family Practitioner (FP)/General Practitioner (GP) for patient-care in Canada (CMA Physician Workforce Survey 2017) [17]

Using digital ledger technology can improve the accessibility of patient data to researchers and healthcare professionals. Seeing as blockchain is a digital ledger technology that can distribute and decentralize information efficiency, health information is available across disparate systems in a more secure environment. Also, digital ledger technology provides a secure network that can manage, share, and access sensitive healthcare information. Before building an effective and efficient information system, establishing a network connecting all users is critical.

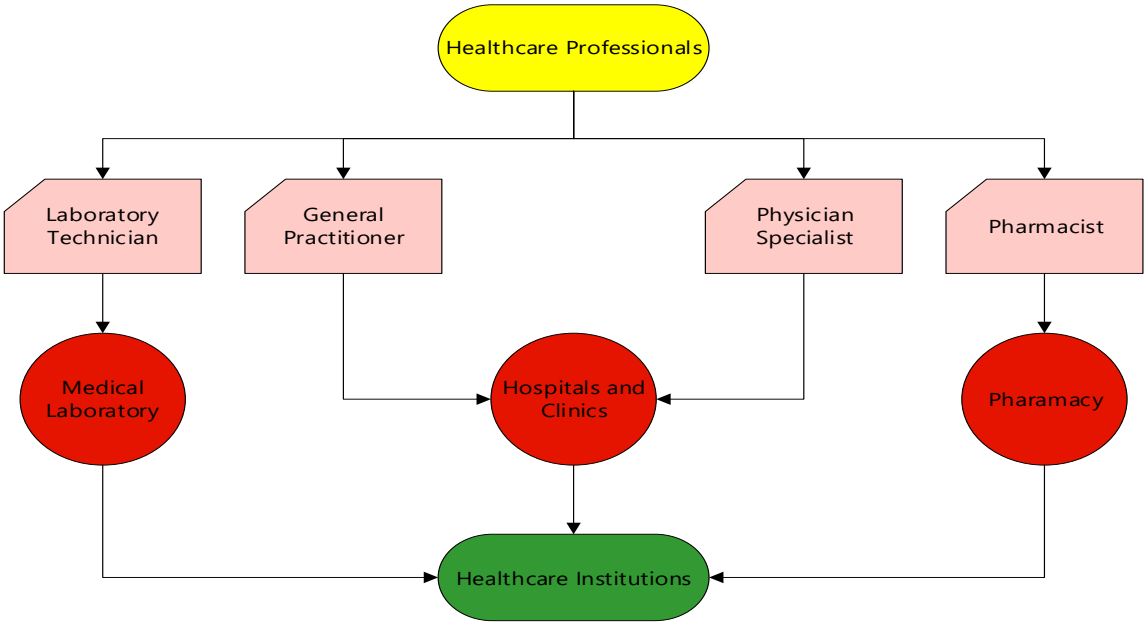


Figure 3 High-Level Diagram of Healthcare Entities and Linkages

Moreover, tracing linkages between hospital professionals and hospital institutions is essential for providing information to organize the requirements of the information-sharing system. Figure 3 presents a comprehensive list of entities as well as attributes for each entity. Examples of entities discussed in Figure 3 include healthcare institutions and healthcare professionals.

In Canada, patient health information is stored by hospitals, clinics, laboratories and pharmacies in their local databases where the patient's treatment is conducted. Thus,

in publicly funded health institutions, patients have the right to access medical records. In contrast, patients that are treated by non-government owned health institutions, for example, private clinics and unregulated health practitioners, are legally exempt from providing patients with access to their medical data.

Additionally, government institutions can actively control, manage, and govern how both patients and healthcare professionals access health data. Currently, medical data is not easily accessible due to the laws governing privacy. As a result, laws on handling, storing and accessing patient medical information vary between provinces in Canada.

Currently, many hospitals use a medical record system to share and access patient health information. However, most health care providers lack the resources to share and access patient medical records across a single network. For instance, in 2018, three major medical facilities located in Ottawa, Ontario, are investing in a new shared medical record system provided by EpicCare Systems [19]. The costs of implementing the system are around $87 million over the next seven years [20]. As a result, implementing a new medical record system is costly. However, the benefits of the share system will save health care professionals time and help save lives.

With over 300 EMR software available and used within various hospitals and clinics around Canada, creating a single network that will allow each software to communicate is ideal. Medical data in hospitals can be managed better with the use of digital ledger technologies. Blockchain technology can trace the use of medical data of patients to ensure that patients' health data are protected and managed accordingly. Having easy access to medical information can assist doctors in providing better care to patients in a timely and accurate manner. Blockchain can authenticate the identities of healthcare

professionals, which in turn can allow for secure access to patient health information. Thus, blockchain can provide access to the data and information depending on where and when patient medical data is needed. Hence, with many regulations surrounding health data, blockchain can set the boundaries to ensure health data is manageable accordingly.

1.5 Blockchain-based EHR systems around the Globe

Medicalchain is a blockchain-based healthcare system that uses blockchain technology to record and store access permissions of medical data of patients to healthcare providers [22]. Medicalchain uses the Hyperledger Fabric platform, which provides blockchain components such as the consensus mechanism for verifying blocks. Medicalchain uses tokens within the Ethereum blockchain to encourage users to validate transactions. In 2018, Medicalchain announced an agreement with Mayo Clinic, a major not-for-profit organization in the United States that focusses on medical care and research, to explore potential use cases for blockchain technology in the medical field [23].

Many countries in Europe have shown a commitment to adopting blockchain technology to promote trust and protection of personal data. In 2018, the European Blockchain Partnership was launched to provide funding for projects extending for various industries involving healthcare and education, which include the use of blockchain and similar digital ledger technologies [24]. The most notable investment includes the My Health My Data (MHMD) project, which uses blockchain to store and transmit medical data to improve data efficiency, reporting of clinical trials, and facilitating data exchange across multiple stakeholders [24].

1.6 Summary of Research Objectives and Contributions

Based on the market analysis performed above, the main objectives of our research include the following:

- Providing accessibility of medical records to patients electronically in Canada
- Promoting discussion for better health information exchange by increasing interest among patients, doctors and researchers
- Demonstrating the usefulness of blockchain technology and the potential benefits it can bring to the healthcare industry

Presently, blockchain is an emerging technology that is expanding and disrupting industries beyond the financial sector. More importantly, blockchain technology has high expectations to succeed in the healthcare sector as it can provide patients ownership of their medical data by managing digital access rights to medical data.

There are several contributions to the field of health research that our study can provide. Firstly, our study will discuss the benefits and challenges of EMR data applied to blockchain technology. Then we will evaluate the implications of blockchain technology for healthcare users. Lastly, we will highlight areas where blockchain technology can support existing health applications.

1.7 Structure of the Thesis

The literature review section contains more than 40 relevant papers representing a variety of conference papers and peer-reviewed publications on the topic of blockchain technology. There is a total of five sections in the literature review. Each paper reviewed is related to blockchain technology. The sections include 1) Blockchain and Supply Chain

Management, 2) Blockchain and E-Health, 3) Blockchain and EMR, 4) Blockchain in Canada, and 5) Blockchain and Smart Contracts to Share EMR data.

In the comparative analysis section, the contribution of each reviewed paper is evaluated based on six key blockchain features. These features include interoperability storage, security, integrity, functionality, and scalability.

In the gap analysis section, the research gaps, as well as the recurring topics found in the literature review section, are discussed. Next, in the problem identification section, we identify our main research questions. An explanation will accompany each research questions on how our research will improve on existing approaches and explain how our extension will be useful.

In our proposed solution, we provide a conceptual architecture, a detailed technical architecture of our design, design discussion, algorithm design, and implementation details. Lastly, in our evaluation section, we examine our proposed solution by evaluating the functional analysis, complexity analysis, efficiency evaluation, and comparative analysis.

In summation, our paper structure is as follows: Chapter 2 Literature Review, Chapter 3 Problem Identification, Chapter 4 Proposed Solution, Chapter 5 Evaluation and Results, Chapter 6 Conclusion and Chapter 7 Future Work.

Chapter 2: Literature Review

In this chapter, we review 46 relevant papers of which 90% are within the last three years. We write a paragraph for the summary, strengths, and weaknesses for each paper. There is a total of 5 subsections in the literature review comprising of blockchain technology in combination with supply chain management, e-health, EMR, Canada and smart contracts to share EMR data. Additionally, we use a comparative analysis table to compare relevant papers based on six blockchain features including interoperability, storage security, integrity, functionality, and scalability.

2.1 Blockchain and Supply Chain Management

Saveen A. Abeyratne et al. [25] provide an overview of industries and applications that use blockchain technology. The authors note that there is a rapid growth in blockchain applications in the financial, social, and legal sectors. In addition, the authors focus on the paper is to apply blockchain in a supply chain management context. Currently, blockchain technology is an emerging technology that can assist in tracking the manufacturing and processing of products. The authors present a use-case involving the manufacturing of cardboard boxes. A supply chain framework demonstrates the sequence of processes in manufacturing cardboard boxes. Thus, implementing the use of blockchain technology allows for information such as the quality of the cardboard boxes to be updated more efficiently at each step in the supply chain.

A strength of this paper [25] includes its effort to outline the importance of transparency in the manufacturing of products. The authors present examples of how supply chain visibility is a challenge for many successful companies. As a result, most companies rely on third-party organizations to ensure the following of regulations and

standards in the manufacturing of a product. Likewise, another strength in this paper includes providing background information on blockchain technology and its technological advantages. A weakness of this paper [25] includes the lack of in-depth research on the drawbacks of using blockchain technology with the manufacturing of products in a supply chain. Hence, as blockchain technology provides transparency and the sharing of validated information, implications surrounding standardization present a concern for companies unable to producing high-quality products.

Zhi Li et al. [26] introduce the concept of open manufacturing, which represents the sharing of knowledge and services among manufactures through the use of blockchain and edge computing technologies. The authors propose a conceptual framework presenting a 6-layer architecture that collects, processes, stores, and shares data between manufacturers. In addition, the authors implemented the open manufacturing conceptual framework in a case study on a Chinese based company that develops and manufactures tire mould. Using both the blockchain and edge computing technologies, companies that operate within the same supply chain can easily exchange knowledge and process information in a secure and distributed network.

An advantage of this paper [26] includes the pairing up of two technologies to facilitate better the sharing of knowledge and services between companies in the manufacturing industry. The authors mention in the paper that the purpose of utilizing these technologies is to provide standardization to implement an open manufacturing methodology effectively and to allow the sharing of valid information within a secure environment. A weakness in this paper [26] includes the absence of examining current systems in which manufacturers share knowledge and services. Taking into consideration

the quality, effectiveness and efficiency of current systems used in manufacturing applications can assist in improving the implementation of the proposed framework.

In the paper [27], Kshetri, N. discusses the role of blockchain technology and its ability to increase the performance levels of various supply chain activities. The author measures the efficiency of blockchain technology in meeting performance objectives based on the analysis of key supply chain metrics, which include cost, speed, dependability, risk reduction, sustainability, and flexibility. Case studies featuring a wide range of companies including Alibaba and Wal-Mart were evaluated based on their application of blockchain technology in their supply chain.

An advantage of this paper [27] includes the author presenting multiple case studies to determine the effectiveness of using blockchain technology in supply chain management. The cases presented in the paper were selected based on the degree of a company's use of the Internet of Things (IoT) technology and needed to validate the identities of people and resources. Due to the structural approach of the paper, the author sufficiently captures a variety of applications of blockchain technology across different companies situated in various industries. With transparency and security providing the building blocks for blockchain technology [27], a missing component found in the paper involves the lack of discussion about the costs associated with implementing blockchain technology in the supply chain. It is essential to realize that successful implementation of blockchain technology depends on the involvement of various stakeholders and access to proper infrastructure.

In this paper [28], Wüst, K. et al. examine many use-cases where blockchain would be a suitable technical solution depending on the application situation. Use-cases analyzed

in the paper include Supply Chain Management, Interbank and International payments, Decentralized Autonomous Organizations and other use-cases. In addition, the authors provide a comparative analysis between blockchain technology and a centrally managed database.

An advantage of this paper [28], includes the authors' proposed methodology for identifying blockchain as an appropriate technical solution. Additionally, the authors presented a flow chart outlining factors including relationships between individuals and application requirements that determine whether blockchain is a feasible technical solution. A drawback of the paper [28], includes the lack of references and statistical pieces of evidence describing the use of blockchain technology. Suggestions about other use-cases involving blockchain technology can provide better support through citing relevant sources.

In this paper [29], Tian, F. constructs an agriculture and food traceability system that uses radio frequency identification (RFID) tags in combination with blockchain technology to help food markets improve the quality and safety of food. As discussed in the conceptual framework, RFID tags collect and share data across the agri-food supply chain. Additionally, blockchain technology validates the data shared and publishes the data in a traceability system.

An advantage of this paper [29] includes the authors' analysis involving the pros and cons of using RFID tags and blockchain technology in an agri-food supply chain. The pros of using these technologies include improved tracking and credibility of food products. The cons involve the high costs needed to support these technologies. Based on the case study presented in the paper [29], RFID tags and blockchain technology can

provide a feasible solution to reduce the agri-food loss ratio and other challenges presented in the Chinese food market. However, seeing as current Chinese agri-food supply chain systems are underfunded and have a lack of resources, applying these technologies requires substantial investments and considerable infrastructure to assist the demanding logistics processes.

Papers	Industries	Examples	Functions
• [28]	• Banking	• Money transfers and loans.	• Blockchain can provide secure and undisclosed money transfers.
• [25], [26], [32]	• Manufacturing	• Cardboard boxes, paper, and printing.	• Blockchain can trace the manufacturing process.
• [27],	• Retail	• Clothing and delivery fulfillment.	• Blockchain can record of product information.
• [29]	• Agriculture	• Food, beverages, and medicine.	• Blockchain can verify the credibility of goods.
• [31]	• Real Estate	• Registering land and properties.	• Blockchain can record and authenticate ownership of residential properties.

Table 3 Comparative Analysis of Uses of Blockchain in a Supply Chain Context

This research paper [30] discusses the integration of blockchain technology with business to business (B2B) transactions based on digital supply chains (DSC). The authors explore the role of DSC in B2B supply networks. Also, the authors use a case study approach to analyze the integration between blockchain technology and DSC.

Korpela, K. et al. key contribution in the paper [30] involves using the quality function deployment (QFD) method to study the integration process between blockchain technology and DSC. The authors' use of focus groups allowed for in-depth results outlining the integration of DSC with blockchain technology. A drawback in the paper, as

mentioned by the authors, includes the research process representing companies solely based in Finland.

In this paper [31], Zheng, Z. et al. analyze the opportunities and threats of blockchain technology by conducting a comprehensive study about the structure, applications, and development of blockchain across various industries.

The authors' vital contribution in this paper [31] includes a detailed analysis of the structural and technical aspects of blockchain. Also, the authors were able to distinctly compare several properties of blockchain as well as potential use cases. A setback in this paper includes its over-approximation of use-cases using blockchain.

In this paper [32], Li, J. et al. focus on the challenges and opportunities facing applications adopting blockchain technology. The authors also develop a framework for implementing blockchain technology in the construction industry, highlighting applications involving smart energy and smart government.

A strength in this paper [32] includes the assessment of the technical, social and political aspects of implementing blockchain technology in the construction sector. A weakness in this paper includes the lack of information on addressing the implementation of a distributed ledger technology.

2.2 Blockchain and E-Health

Fran Casinoa et al. [33], paper present a comprehensive analysis of blockchain technology. The authors explore a variety of applications of blockchain by discussing trends, limitations, and research gaps found in different industries related to financial, government and business.

The main contribution of the paper [33] is the authors' research regarding various papers focusing on blockchain-based applications. Approximately 260 research papers published between 2014-2018 were analyzed. A setback in this paper includes the lack of detailed information in the analysis of blockchain versus traditional databases.

In [34], Castaldo, L. et al. explore the importance of eHealth in Europe and the practice of exchanging patient healthcare information between two countries. Moreover, this research paper proposes a log management system that provides traceability and authenticity operated on blockchain technology.

This paper [34] provides an improvement for managing the current logging system used for cross-border data exchange of eHealth in Europe through the implementation of the KONFIDO project. Additionally, this paper outlines in-detail the infrastructure of the logging system as well as its integration with several technologies of which includes blockchain. A disadvantage of this paper [34] includes its narrow focus on the transfer and storage of data within the flow logs. Additional analysis of the features and costs of these technologies would provide a more in-depth approach.

This paper [35] outlines the security and privacy issues regarding consent management in the E-Health sector. Moreover, the authors consider blockchain as a suitable technology that can manage the consents of patients with their healthcare information.

Genestier, P. et al. key contribution in this paper [35] includes a use-case diagram that describes the process of monitoring patients' consents while using blockchain technology. A drawback in this paper [35] shows insufficient evidence on patients having issues with managing the consents of their medical data. The authors mention that hacking

and privacy violations are the main issue. However, there is little to no research displaying patients wanting to control their medical data.

This paper [36] discusses topics on blockchain technology, benefits of blockchain for biomedical and health care applications, and potential challenges of adopting blockchain in the healthcare industry.

Papers	Digital Health Topics	Description	Examples	Benefits
• **[34], [35], [36], [38], [40] - [44],**	• Electronic Health Records (EHR)	• Managing patient health and medical data.	• Patient demographics • Medical history	• Improve the accessibility of patient data.
• **[37], [39], [47], [48], [52], [53]**	• M-Health	• Healthcare services provided via mobile devices.	• Telemedicine • Mobile health applications	• Provide a cost-effective and convenient tool for accessing health information.
• **[65]**	• Smart Healthcare Systems	• Using smart technology to analyze and predict a patient's health.	• Health monitoring visualization • Real-time information about patients	• Increase the effectiveness and productivity of healthcare processes.

Table 4 Comparative Analysis of Uses of Blockchain in E-Health

The main contribution found in this paper [36] includes Kuo, T. T. et al. detail analysis of features and current applications in the blockchain. Also, the authors outline critical use-cases for adopting blockchain technology in the healthcare field. Some of these use-cases include medical record management, insurance claims process, and clinical medical research. A disadvantage of this paper [36] includes its lack of focus on

introducing a new application of solving the challenges with implementing blockchain technology in the healthcare sector.

In [37], Ahmed, T. et al. provide an overview of electronic health and mobile health systems in Bangladesh. The report offers insights into the challenging relationships between the government, healthcare sectors and telecommunications services. The study further explores various e-health and m-health initiatives as well as users' behaviour on health services.

Ahmed, T. et al. contribution in this report are evident in its examination of a use-case involving the opportunities and challenges of e-health and m-health. The authors provide substantial evidence about trends in the spreading of mobile devices and the accessibility of health information via websites and text messaging. A weakness displayed in the report relates to the authors' assumptions on the dependency of the government to provide a regulatory framework for the use of e-health and m-health services. As a result, there is a lack of information in the report about current plans put in place for the future development of electronic and mobile health systems.

In this paper [38], Mettler, M. outlines the potential of blockchain technology in the healthcare industry. The author provides many examples of ways that blockchain can improve patient care. Some of these examples include utilizing patient-generated health data found in health apps and reducing counterfeit drugs in the pharmaceutical industry.

A strength in this paper [38] includes its use of blockchain technology to benefit and improve patients care. The paper continues to outline the benefits by providing evidence on organizations and healthcare companies implementing blockchain solutions.

A weakness in this paper [38] includes its lack of analysis of the prospective market disturbances and changes in the healthcare industry given the use of blockchain technology.

In this research paper [39], Weiss, M. et al. attempt to address the security challenges associated with mHealth by recommending blockchain technology as an upgraded security model. The paper further examines the legal framework, current mHealth implementations, and other applications of security in mHealth relevant to its use in South Africa.

The main contribution of this paper [39] is the analysis of legal policies and regulations concerning the collection and use of personal information regarding medical data. Also, the authors examine the current gaps in the research and provide benefits of implementing blockchain within mHealth applications. A drawback in this paper is its qualitative approach of summarizing blockchain and mHealth principles.

2.3 Blockchain and Electronic Medical Records (EMR)

Dubovitskaya, A. et al. [40] investigates the significance of using blockchain technology to support the sharing of electronic medical records (EMR) among various sectors in the healthcare industry. The authors perform a framework analysis highlighting the managing of data for patients involved in radiation therapy.

An advantage of this paper [40] underlines the immense opportunity of how blockchain technology could enhance and improve eHealth services. The prototype presented in the paper describes blockchain ability to ensure patients' data are protected, transparent, and easily accessible among a network of trusted healthcare professionals. A disadvantage of this paper includes the absence of discussion about the effects of

blockchain technology changing the communication standards between patients, pharmacies, hospitals.

Bingqing Shen et al. [41], paper proposes a metadata exchange system called MedChain, which attempts to meet security and efficiency standards in data sharing. MedChain uses a decentralized network that connects healthcare providers, patients and doctors. According to the procedures mentioned in the paper, a blockchain network, which stores immutable data such as digital footprints and a peer to the peer storage network, which stores the description of the data.

The main contribution of this paper [41] includes the authors' proposal of a session-based data-sharing scheme that supports data streams from IoT devices, reduces storage space on the blockchain and manages access control of shared medical data. The main setback of this paper is its lack of description of involving data loss/corruption measures when during storage or transmission of health data in the network.

In [42], Azaria, A. et al. propose MedRec, which is a system that uses blockchain technology to manage electronic medical records of patients. The proposed system aims to improve the accessibility of medical data and provide a history of medical transactions for patients and healthcare professionals.

An advantage of this paper [42] includes its proposed record management system utilizing blockchain technology. The authors present a unique method involving incentivizing medical stakeholders to maintain the MedRec system based on an Ethereum model or a smart contract model. A disadvantage of this paper includes the design of the MedRec system as it is based firmly on the Bitcoin application. Hence, alternative

viewpoints of using blockchain technology with electronic medical records continue to be unconsidered.

This article by Samavi, R. et al. [43], explores the opportunities and challenges of developing a blockchain application for healthcare research. Blockchain technology can provide accessibility of patient data in a secure and protected environment. Also, utilizing patient data for research purposes can advance eHealth services by providing better healthcare services for patients. An advantage of this article [43] includes its support of medical research aimed at handling medical data while safeguarding patient personal information. A setback in this article presents discrepancies regarding the storing of patient medical information in the blockchain.

In this paper [44], Rifi, N. et al. propose an architecture that uses blockchain technology to facilitate medical data exchange, as well as access to EMR and EHR. In addition, the authors discuss the use of smart contracts for future applications related to eHealth. A strength of this paper [44] includes its attempt to solve challenges, including the security and scalability of e-Health applications while using blockchain technology. A weakness of this paper is the absence of dealing with the difficulties of using blockchain technology and the effects on the healthcare industry.

In [45], Zhang, X., et al. propose a blockchain-based architecture for managing EMR data. The proposed architecture supports granular access control, which improves the security of patient information stored in a blockchain. An advantage in this paper [45] is in the design of the security access model in which data transportation transpires in the user layer, agent layer, and storage layer. A disadvantage in this paper is that there is insufficient data about current challenges about EMR databases.

In [46], Theodouli, A. et al. propose a blockchain-based architecture that enables the sharing of healthcare data for improving medical research. As shown in the system architecture, patients can share their health data within the blockchain network. Transfers of health data in local databases occur by way of web/cloud services. Subsequently, smart contracts ensure the security and privacy of data sharing.

In the use-case scenario section [46], the authors provide in incredible detail a high-level description of managing requested permissions of data between patients and medical research centers. A weakness in the paper is apparent in the event of a patient sharing data without an account. The absence of an account can significantly reduce the quality of health records shared in the platform due to patient personal information being unverifiable. However, as mentioned in the proposed model, the authors assume that data uploaded by patients are trusted.

In this paper [47], Sofia Alexaki et al. propose a permissioned blockchain application that provides medical records access management using smart contracts. Use cases of this application involve an agreement for managing, viewing, updating and accessing electronic patient records (EPR) by healthcare providers. The authors' contribution in this paper [47] includes the description of the process of a healthcare provider requesting access to an EPR. A drawback in this paper is that it focuses on regulating access to EPR without mentioning the implications of healthcare providers.

Shan Jiang et al. [48], propose a blockchain healthcare information exchange (BlocHIE) system that stores and shares personal healthcare data (PHD) collected by individuals and electronic medical records (EMR) provided by healthcare institutions. To

ensure data privacy and authentication, the authors propose two fairness-based transaction packing algorithms to handle EMR data and PHD data.

An advantage of this paper [48] includes the author's use of off-chain storage and an on-chain verification method to manage EMR data. A disadvantage of the paper includes the lack of description outlining the benefits of storing PHD data provided by patients in the blockchain system.

Tanesh Kumar et al. [49], discuss potential applications of blockchain technology in the healthcare industry. Areas of applications include clinical data sharing, data access control, research and clinical trials, drug supply chain management and others. Also, the authors mention various critical requirements for creating a blockchain-based healthcare system. These requirements include nationwide interoperability, data security, data integrity, cost efficiency, transparency and complexity.

The main contribution of this paper [49] is the discussion of the future scope of blockchain in the healthcare industry. The authors identify significant ideas on how blockchain can provide solutions for improving the storage, interoperability, and security of healthcare data. A setback in the paper is the exclusion of comparing blockchain with other technologies that have similar properties.

Peng Zhang et al. [50], the paper analyzes blockchain healthcare decentralized applications based on several key metrics. Examples of metrics used include policy compliance, authentication, interoperability, scalability, patient-centered, and others.

An advantage of this paper [50] is that it presents a guideline for evaluating blockchain healthcare applications. A disadvantage of this paper is the lack of evaluation of using the criteria proposed in real use case examples.

Xiaochen Zheng et al. [51], the authors propose a blockchain architecture that utilizes cloud storage and machine learning practices to share health-related data between individuals securely and transparently. In the proposed blockchain architecture, reasons for sharing healthcare data are for medical, research and commercial purposes.

A strength in this paper [51] is in the conceptual design of the blockchain system. The authors assign an application for each role in the system. Thus, each application has different functionalities for different roles. Also, all applications integrate efficiently within the blockchain network. A weakness in the paper [51] is the use of public key infrastructure for managing health data. It is important to note that sharing personal data for reasons other than health-related services can reduce the quality of information.

You Sun et al. [52] propose a decentralized attribute-based signature scheme (DABS) for sharing electronic health records (EHR) across many Care Delivery Organizations (CDO). The proposed system will provide an on-chain and off-chain storage system that can secure and verify EHR data shared within the network.

An advantage of this paper [52] is evident in the analysis of security measures proposed within the proposed DABS algorithm. Security aspects discussed include unforgeability, anonymity and security under a collusion attack. As a result, each security aspect implements attributes to verify and identify the user identity in the network. A disadvantage of this paper is apparent in the limited information provided about the off-chain storage of EHR of patients.

David Randall et al. [53], examines the use of blockchain applications in the domain of health information systems. The paper studies current public record management systems and the potential of blockchain to reduce costs linked with health information.

A strength found in this paper [53] is the analysis of the U.S. Medicaid and Medicare systems. The authors expertly explain the implementation process of adopting an electronic healthcare system by outlining the successes and setbacks of the U.S. healthcare system. A weakness found in the paper is the lack of study of the implementation costs of the use of a blockchain application.

Hoger Mahmud et al. [54], propose a conceptual model to address record verification and verification using blockchain. The authors proposed model is specific to virtual healthcare systems and uses a virtual breeding environment (VBE) and virtual organization (VO) framework. VBE is used to verify information about healthcare providers and VO is used to provide healthcare services to patients.

The main contribution of this paper [54] is the creation of a virtual healthcare system that records, verifies, and validates health data efficiently using blockchain, VBE, and VO technology. The potential benefits of this proposed framework can minimize transactional costs and ensure that up-to-date healthcare information available across all service users. The main setback of this paper is the storing of health records on the blockchain. The authors have not identified information regarding what specific health data that is on the blockchain.

2.4 Blockchain in Canada

Bobby Gheorghiu et al. [55], examines the proposal of an interoperable electronic health records (iEHR) system in Canada. iEHR provides a wide-range view of a patient's medical history within a network. The authors examine the deployment and use of a fully integrated iEHR system for patients living in Canada.

An advantage of this research article [55] is that it provides statistics and analysis of measuring the use of iEHR systems. The authors outline that there is an increase in the number of active users of iEHR systems in Canada. A disadvantage of this paper is the lack of recommendations surrounding decisions for the better management of interoperable EHR adoption.

Sukirtha Tharmalingam et al. [56] research article studies the processes of exchange health data between clinicians and patients. The authors analyze survey responses that are evaluated based on user perspectives, system and service quality, information quality, user satisfaction, productivity, and quality of an iEHR system.

A strength in the paper [56] is that it measures the value of iEHRs from the perspective of their users. As a result, the authors were able to provide unique insights about shared patient information accessed daily. A weakness in the research article includes the analysis of data taken from 2006 to 2014. Hence, data studied may not reflect the current healthcare landscape of EHR in Canada.

Thorsten Koeppl et al. [57], provide an in-depth study on the economic impact of blockchain technology in the Canadian financial market. The authors discuss the opportunity of blockchain to provide interoperability between federal, provincial and municipal levels of government. Potential applications of blockchain technology in the Canadian market include payment systems, smart contracts, corporate governance, financial markets, and government services. In addition, various dimensions of blockchain are addressed based on their given benefits and challenges. These dimensions include safety, efficiency, incentive verification, and technology development.

An advantage of this paper [57] is the authors' analysis of the policy and regulatory challenges of implementing a new technology such as blockchain. Aspects of blockchain that can be affected by policies include data management and network connectivity of public and private infrastructures. A disadvantage of this paper is the lack of evidence identifying a cost-efficient solution of implementing blockchain technology in the Canadian market.

Greg Wolfond [58], paper explores the use of blockchain technology to improve service delivery in the public and private sectors. Blockchain can provide a secure method to identify, verify and share personal information digitally. The author mentions that having secure digital identities will improve accessibility to government services and healthcare management in Canada.

A strength in this paper [58] is the continuing theme to promote digital services that connect individuals and service providers in a more secure and privacy efficient way. As a result, blockchain technology can provide a secure network to which data can be accessed, viewed and shared efficiently. A setback in this paper is a lack of information surrounding the impact of blockchain on the Canadian economy.

Amitha Carrnadin research paper [59], provides an overview of the healthcare market in Canada by discussing challenges and opportunities of electronic healthcare records (EHR). Also, the author presents an overview of blockchain technology by mentioning its limitations, legal considerations and barriers of use with EHR of patients. Lastly, Amitha provides recommendations regarding utilizing blockchain in the healthcare sector.

An advantage of this paper [59] is the recommendations for the healthcare sector in Canada. Amitha mentions the importance of increased standardization to enhance the use of EHRs. Also, Amitha recommends that the public healthcare sector will benefit by collaborating with private technology firms to find cost efficiencies regarding blockchain technology and to assist in providing improve medical services to patients. A disadvantage of this paper is the lack of discussion of other technologies that can assist in overcoming the barriers to EHRs.

Evangeline Ducas et al. [60], provide a summary of the technical capabilities of blockchain technology and its opportunities in both financial and government sectors. The authors explore the regulatory concerns and approaches that will assist in enabling the adoption of blockchain within Canada.

The authors' key contribution of this paper [60] involves the analysis of the economic, financial, regulatory and consumer influence for blockchain. The authors recommend that Canada implements a regulatory sandbox model to engage new business models to support new technologies including blockchain. A disadvantage of the paper is the number of suggestions for further research resulting in many unanswered questions regarding the influence of blockchain technology in Canada.

2.5 Blockchain and Smart Contracts to Share EMR Data

Javier Munster et al. [61] address the security concerns with publish/subscribe messaging by using a secret sharing scheme, a trusted service, and a hybrid broker network. To share secret information between publishers and subscribers, the authors propose a model named HyShare. To adequately share secrets, HyShare attempts to reduce the number of steps to share a single secret.

This paper [61] encompasses the importance of confidentiality of sharing data in a network. As a result, the authors examine the performance metrics of HyShare based on the number of secrets, the number of fragments, and the number of messages sent in the system. Another advantage of this paper includes highlighting the importance of a trusted system broker to facilitate messages sent across a network. Thus, secret sharing of data will expand as technology evolves in the future. In contrast, a disadvantage of this paper is the constraint of using a third-party software to share a secret. As technology becomes widely available, this will reduce the reliance on third-party software.

Kshetri N. paper [62] analyzes the challenges related to cybersecurity and privacy of data with current IoT systems in comparison to blockchain-based solutions. The paper also covers various technologies, including blockchain and cloud computing, given their roles in enhancing IoT systems regarding security with access management systems, improving the tracing of IoT devices, and impose public policy given the use of smart contracts. Also, the paper demonstrates the opportunity of blockchain technology to strengthen the security and privacy of patient data regarding digital health.

A strength in this paper [62] is in the comparison of security and privacy concerns found in cloud computing and blockchain technology. The criteria used to compare each technology are efficiency, cost-effectiveness, deployment, cybersecurity, and key challenges faced. A weakness found in this paper is the lack of examples of the wide-use of health-based blockchain systems. However, as blockchain is a developing technology, the drawbacks of security and privacy of data shared can be minimized in the long-run.

Sergey Novikov1 et al. [63] presents a blockchain health care infrastructure to manage the secure storage of data. The authors propose an algorithm that utilizes smart

contracts for storing and securing electronic medical records. In addition, the authors introduce an integrated electronic medical record (IEMC) as a system that will facilitate e-Health services, including telemedicine, medical analytics, mutual settlements for medical care and other services. The algorithm proposed allows patients to give temporary access to their medical data through a smart contract that also defines the interaction between the doctor and the patient.

An advantage of this paper [63] includes the authors' mention of unresolved issues of blockchain technology comprising of maintaining data quality, standardizing medical data, and integrating data processing with current healthcare systems. This paper could provide more discussion surrounding the advantages and challenges of blockchain technology concerning non-key stakeholders such as insurance companies, pharmacies, research organizations, supervisory bodies, and public service delivery systems.

Kristen Griggs et al. [64], use blockchain-based smart contracts to support patient monitoring by managing the transferring of data of various medical sensor devices. The process of transferring data is as follows. The data obtained from sensor devices will be formatted and managed by a smart contract. The use of smart contracts will allow data to be processed based on set parameters outlined within the smart contract. Additionally, the authors recommend managing the security concerns of medical data transferring by maintaining privacy and control of data stored on the blockchain.

A strength of the paper [64] includes the authors recognizing the challenges of increasing response time. A prerequisite of adding a new block to the blockchain requires the verification of the previous block. Thus, achieving consensus within the blockchain could require significant time depending on factors involving the storage of each node and

the overall size of the chain. A drawback of this paper is the assumption of data security through the encryption of IP protocols. Although effective encryption can reduce most security vulnerabilities, automating health notifications can be a complex problem due to the predefining of conditions.

Peng Zhang et al. [65], explore the capabilities of blockchain technology with an emphasis on smart contracts to deal with the interoperability challenges facing healthcare applications. The authors discuss the role of smart contracts in assisting in the minimization of integration complexities, reducing data storage requirements, and balancing integration ease with security concerns. Likewise, the authors propose a decentralized application for smart health (DASH) to improve healthcare interoperability.

The main contribution in this paper [65] is that the authors attempt to tackle the challenges of interoperability when designing a healthcare architecture by reducing computation and storage costs. Hence, applying software patterns including abstract factory, flyweight, proxy and publisher-subscriber were effective in addressing some of the design and scalability challenges affecting interoperability. Despite the contributions of software patterns, the lack of scalability of blockchain remains a significant implementation challenge. Thus, discussing alternative approaches other than software patterns can provide more depth in understanding the interoperability challenges in blockchain-based healthcare applications.

Olivia Choudhury et al. [66], propose a framework using blockchain to design smart contracts to meet the regulatory requirements for data collection, data sharing, and consent management. The authors discuss the implementation of a permissioned blockchain system while citing the Hyperledger Fabric as a private blockchain framework.

A strength of this paper [66] is evident in the proposed blockchain-based system. The authors were able to implement the guidelines for accessing, consenting, sharing, and storing health data among patients, healthcare professionals and research organizations. Nonetheless, smart contracts provide a method to enforce regulations towards achieving effective data management. Assessing the scalability of a blockchain system will provide more development for smart contracts to be utilized differently in creating better strategies for data management.

Huanrong Tang et al. [67] propose a model for the secure sharing of medical data, specifically medical images, based on applying smart contracts. This proposed model will also use a credit score mechanism to manage data permissions between patients and hospitals. The authors emphasize cross-domain sharing as well as patient privacy protection. A strength of this paper [67] includes using smart contracts to enable communication between different medical institutions within a shared network. Conversely, patient privacy can be improved with additional mechanisms to perform verification and protection of patients' medical data.

Yining Hu et al. [68] paper presents an overview of the use of smart contracts in various applications. Potential use cases of smart contracts concerning healthcare include digitizing health data, patient identification, and personal health tracking.

A strength in this paper [68] includes the authors' recognition of potential challenges limiting the advancements of smart contracts in the healthcare industry. To point out, the authors mention security, regulation, user acceptance, and scalability to be significant challenges. On the contrary, this paper can gain from discussing areas to reduce development costs for existing smart contracts applications.

Bo Li [69] thesis paper investigates blockchain and smart contracts to support personal data management. In the proposed architecture, smart contracts provide a trusted environment to assist users with accessing and utilizing their data. Additionally, the author introduces a case study involving a physical therapist collecting data from patients for research purposes. The author aims to establish a transparent environment that allows patients to share personal data with doctors and research organizations.

A strength in this paper [69] involves the comparison of various frameworks including AWARE and MyData, that are user-friendly and do not require extensive knowledge of coding. A drawback of this paper includes the selectiveness of storing data on mobile devices. A possible way to extend this research is to consider various human-centric approaches to include more internet-connected devices.

Jonatan Bergquist [70] thesis paper explores the domain of privacy-sensitive applications for electronic medical records (EMR) built using blockchain technology and smart contracts. The author examines the development of a blockchain application that meets the storage requirements of prescriptions for patients and permits patient privacy data sharing.

A strength of this paper [70] includes areas of discussion on the topics consensus protocols including the proof-of-work, proof-of-stake, proof-of-validation and proof-of-authority. In addition, the authors use smart contracts to facilitate the interactions between the patient, doctor and pharmacy. As a result, information including prescriptions, patient information and pharmacy identity require sharing permissions provided by the blockchain. A drawback of this paper is the adoption of the by government and in terms of

scalability. Considerable research is needed to support the implementation of this system through government agencies.

Ravi Kiran Raman et al. [71], construct a ledger using a hash chain structure that provides security, integrity, and confidentiality of data stored in the blockchain. The authors present an adversary model for targeting denial of service (DoS) attacks and targeted data corruption attacks. The proposed coding scheme in the paper helps facilitate distributed secure storage.

An advantage of this paper [71] is the presenting of various algorithms for the recovery of stored data in the blockchain. As a result, adversaries cannot steal user identities or corrupt the data stored in the blockchain. In contrast, a setback of this paper includes the lack of a use-case study.

Paper	Approach	Application	Interoperability	Storage	Security	Integrity	Functionality	Scalability
[25]	Manufacturing	Manufacturing Supply Chain	Without using a third party, data can be entered and shared.	Users of the network must have technical capabilities to store and manage data.	Mining to improves security by validating transactions added in the blockchain.	Verifying information stored on the blockchain can be costly. However, users can be confident and trust information stored on the blockchain.	The blockchain system will function as designed based on the established system protocol.	Collaboration with government, research and industrial organizations will improve the scalability of blockchain technology.
[26]	Manufacturing	Sharing Services and Information for Manufactures	Providing a network that includes customers and companies connected through contracts.	Uses edge computing to process and store data not stored in the blockchain.	Data encryption on the blockchain allows data exchanges to be anonymous.	Blockchain allows for more accurate record-keeping while ensuring transparency of ownership.	The nodes in the system maintain data blocks. Once data is verified, it is added to the blockchain and permanently stored.	Blockchain allows development and scalability for businesses while maintaining cost-efficiency.
[27]	Internet of Things (IoT)	Supply Chain Management	Blockchain allows each user to see and share data with other users.	Blockchain provides a secure storage mechanism that validates the identities of users and digitally signed documents.	Users on the blockchain network identities are confirmed, allowing for the tracking of time and location of each transaction.	Supply chains can assess the quality of resources more accurately by the tracking and verification mechanisms provided by blockchain technology.	Blockchain has the flexibility to improve supply chain performance, given a small number of users.	Determinates of blockchain scalability can be due to the capabilities, competitiveness based on the number of users involved.
[28]	Multiple Approaches	Supply Chain Management	Blockchain allows mistrusting users to interact, trade and exchange financial data without the need of a third party.	A blockchain is suitable for supply chain management applications as multiple users and nodes contribute to the storing of data.	The security of a blockchain system is dependent on the verification mechanism.	Unauthorized users cannot alter the integrity of information stored on the blockchain.	Transparency and verification are requirements for blockchain systems to function.	The scalability can vary depending on the number of users and updates the blockchain system can handle.
[29]	Agriculture	Supply Chain Management	Data can be exchanged and shared anonymously in a traceable environment.	Proper storage management in an agricultural environment is essential for tracking important information such as delivery time.	Using blockchain removes the need for a centralized system.	A consensus among the blockchain users is needed to reduce data tampering and provide a high level of integrity.	Radio Frequency Identification (RFID) is used along with blockchain to provide food safety and transparency of the supply chain.	The scalability of blockchain is immature, seeing as the capacity of transactions is restricted to 7 per second.
[30]	Business to Business (B2B) Integration	Supply Chain Management	Data standardization is needed to integrate digital supply chains between various organizations.	Supply chains must support the integration and storage of information between multiple systems.	Blockchain provides tools such as smart contracts to enable secure transfers of data.	Blockchain reducing the use of intermediaries results in increasing data integrity.	A list of functionalities provided by blockchain includes transactional processing data, the use of smart contracts, storing blocks in a peer-to-peer network, and managing blocks through miners.	Scalability concerns of blockchain include interoperability within systems, monitoring the system, real-time tracking of data, and user identification.
[31]	Multiple Approaches	Internet of Things and Smart Contracts	Blockchain can provide a decentralized environment for exchanging data without the need for a third party.	Storage optimization is needed as large blocks can decrease the speed of transferring information in the network.	Blockchain can use public key infrastructures to exchange sensitive data securely.	Data integrity is preserved through the use of a reputation system to measure the trust of users.	The use of smart contracts can increase the functionalities of blockchain.	Storage optimization and redesigning of blocks are the key scalability concerns for blockchain.
[32]	Multiple Approaches	Assessing Blockchain's Social, Environmental, and Economic Impacts	Data accessed through blockchain must be standardized by sharing requirements found from one application to another.	Data storage occurs across many computers/nodes in the network.	Data stored on the blockchain is immutable.	All blocks in the blockchain must link to the previous block in the chain.	The use of blockchain can provide quality assurance by reducing human error.	A reliable internet connection can improve the stability and scalability of a blockchain system.

[33]	Multiple Approaches	Supply Chain Management	Blockchain can provide secure and audible data exchange. Also, blockchain can incentivize entities to facilitate data exchange.	Data storage optimization reduces the number of transactions and block size in a node allowing for faster verifiability of transactions.	Security and privacy of information stored on a blockchain are high versus traditional databases.	IP protection can increase the integrity of a blockchain system.	Smart contracts can advance blockchain applications to store and update data dynamically.	A proof-of-stake protocol can increase the integrity of a blockchain system.
[34]	E-Health	E-Health in Europe	The KONFIDO project will provide cross-border interoperation of eHealth services within Europe.	Blockchain can utilize a multichain system that stores data in every node in the system.	Data security is through symmetric and asymmetric encryption.	Time-stamping and public keys provide data integrity and confidentiality.	Multichain blockchain does not rely on the proof-of-work mechanism to verify transactions.	Private blockchain system can increase the chances of large-scale adoption of blockchain technology.
[35]	E-Health	Consent Management in E-Health	Blockchain technology implements the consent management of patient data.	Patient data is available in the data management server. Blockchain records authorization transactions.	The Hyperledger blockchain platform provides security management of patient data.	Government regulations enforce data integrity and privacy.	Blockchain provides features such as managing the access of patient data from trusted third parties.	Many users are needed to support the scalability of the proposed system.
[36]	Biomedical and Healthcare	Improved Medical Record Management	Through blockchain, patients own and control their health data. Also, patients can share their health records with other healthcare providers.	The storage of health data of patients is in a private blockchain.	The blockchain network denies unverifiable health data.	Health data is decryptable only using the patient's private key.	Storing patient health information in the decentralized network reduces the hackability.	The speed of blockchain can provide a concern when dealing with the sharing of real-time data.
[37]	M-Health	M-Health application in Bangladesh	Use of smartphones to connect healthcare professions and patients.	Opportunities include collecting and distributing data through online databases.	Development ideas include a real-time data backup system.	Confidentiality and privacy concerns are a challenge for M-Health.	Text-based health campaigns can be sent messages without additional cost.	The relationship between telecommunication companies and health institutions concerning regulatory issues will determine how well blockchain technology is scalable.
[38]	Healthcare Industry	Healthcare Management Applications	Examples of healthcare management applications include a data trading network for patients, a network for healthcare specialists and a supply chain system to manage prescription drugs.	Patients can store and manage personal healthcare data in their application.	Healthcare data stored using blockchain are secure.	Healthcare data is shared directly using blockchain.	Blockchain can reduce costs for hospitals, benefit patients in the long-run, and decreasing the market for counterfeit prescription drugs.	Blockchain provides the ability to improve interactions in the health sector, given the avoidance of data intermediaries.
[39]	m-Health	Security Challenges in m-Health	Enterprise Mobility Management Platforms (EMMP) are used to address interoperability issues relating to a large number of mobile devices.	Blockchain will store transactional data regarding ownership.	Data on the blockchain can support m-health applications for public health services.	Digital signatures protect the integrity of medical data.	Public m-Health applications are risky and costly to maintain.	A large number of mobile health applications available demonstrates growing interests for m-Health services.
[40]	Electronic Medical Records (EMR)	Data Management in Radiation Oncology	Patients can choose to share some parts of their medical data. Blockchain can keep track of shared medical data between patients and doctors.	Cloud-based storage will store patient medical data. Also, the storage of metadata, taken from patient medical data, is on the blockchain.	Security capabilities of blockchain include cryptographic functions such as hash, asymmetric encryption and digital signature.	Secret keys and hash functions ensure data security by encrypting medical information of patients.	Doctors can request permission to upload patient health data permitted by the patient.	The scalability of the proposed framework for sharing patient data is unexamined.
[41]	Healthcare Industry	Healthcare Data Sharing	Cryptographic keys assist in exchanging data between healthcare services and patients.	Managing mutable information on the blockchain is inefficient as more storage spaced is consumed.	Secrecy protocols help reduce security attacks in the blockchain system.	Data stored on the on-chain is immutable, and data stored off-chain is corruptable.	Data stored on the blockchain is tamper-proof. Off-chain can be generated, produced, and removed.	System latency is a concern given the number of off-chain directory nodes.

[42]	Electronic Health Records (EHR)	Electronic Medical Record Data Management System (MedRec)	MedRec attempts to reduce the challenges of interoperability for patients, providers, and health institutions by encouraging open standards for health data exchange.	The storage of medical records is on local servers. Copies of authorization data are in each node in the network.	The proof-of-work algorithm secures medical records from tampering.	Identify confirmation is via public key cryptography and using a DNS distributed database implementation.	Patient local databases will store a patient's medical data. Missing data can be from the blockchain network.	A higher number of transactions can affect the performance of MedRec. A large scale of health data management system requires further development.
[43]	Healthcare System	Real-time Access to Patient Data	Blockchain will be able to support the access of data in collaborative health research.	It is impractical to store health records on a blockchain. Hospitals currently store patient data.	Blockchain will be able to provide timely and secure access to medical data to researchers.	Blockchain will provide collaboration between untrusted parties, including patients, researchers, and hospitals.	The design of the system must facilitate collaboration between users and data providers while adhering to privacy policies surrounding data accessibility.	The scalability of blockchain-based solutions will require approval from multiple authoritative bodies.
[44]	Electronic Medical Records (EMR)	Medical Data Exchange	Doctors, hospitals, patients, research centers, and insurance companies can connect privately and securely through blockchain.	An InterPlanetary File System (IPFS) provides an off-chain storage system.	Smart contracts secure data exchange between patients and doctors.	Privately secured data allows patients to control their medical data.	IPFS and cloud computing can be used in collaboration with blockchain to improve the performance in the network.	Examining parameters such as latency, throughput, and the size of the blocks can ensure scalability.
[45]	Electronic Medical Records (EMR)	Security of Patient Information	Shamir's Secret Sharing will provide data access control when sharing patient information on the blockchain.	Storage of EMR's are in the blockchain.	Health care records are secured using keys, enabling access control.	Integrity checks are implemented based on the Advanced Encryption Standard (AES) algorithm.	Comparisons of cryptographic operations and computational time efficiency are evaluated.	Scalability is unconsidered, given the storage of all EMR on the blockchain.
[46]	Electronic Health Records (EHR)	Sharing Healthcare Data	A consensus algorithm called proof-of-interoperability is suggested based on the Fast Healthcare Interoperability Resources (FHIR) protocol.	Web-hosted, or cloud services, store patient health data.	The cloud server stores hashed health data.	The requesting entity must match the hashed data stored on the smart contract to access the data.	Request permissions allow for easy access to healthcare data by research centers while ensuring patient privacy.	The proposed system can be scaled to adapt to the KONFIDO project.
[47]	Electronic Patient Records (EPR)	Medical Records Access Management	Sharing patient records is uncommon seeing patients and health institutes have their workflow, trust, and privacy parameters for medical data.	Data stored on the blockchain must meet to minimize storage requirements and be interpretable universally.	Records access management requirements are applied to allow or prohibit access to patient data.	Blockchain assists in providing data integrity by allowing patients to obtain complete control of their data.	Additional off-chain applications are needed to offer better functionality to all blockchain participants.	Scalability is dependent on the jurisdictions provided by government authorities regarding public health.
[48]	Electronic Medical Records (EMR)	Information exchange system (BlocHIE)	BlocHIE system architecture allows for health information exchange (HIE) between hospitals and patients through a blockchain network.	BlocHIE provides off-chain storage of EMR data.	To keep confidentiality and privacy, the detailed medical record of a patient is not publicly accessible.	Requirements including privacy, authenticity, throughput, latency, and fairness can determine the sharing and publishing of patient medical records.	Each submitted transactions must be validated before added to the blockchain.	The hash value, comprised of a few kilobytes, is stored on the blockchain.
[49]	Healthcare Industry	Blockchain and Smart Contract-Based Healthcare Systems	Nationwide interoperability is a significant obstacle to healthcare management systems. Blockchain has the potential to provide safer and more efficient data sharing.	Blockchain can assist in maintaining and storing medical records.	Data accessibility and security remains to be a significant challenge, as all users are aware of transactions shared within the blockchain system.	Blockchain can help support data consistency, and feasibility as data stored in blocks are immutable.	Overall, blockchain can improve, enhance, and provide better quality healthcare services.	Computer capabilities and the number of medical transactions performed can reduce the scalability of healthcare-based blockchain solutions.
[50]	Healthcare Industry	Decentralized Applications in Healthcare	Requirements for efficient interoperability include HIPAA compliance, user authentication, and cost-effectiveness.	Patient data stored in the blockchain is encrypted and anonymous.	Security involving authentication and recovery of lost or theft information has the potential to be improved on the blockchain.	There is a lack of trusted linkages connecting independent health systems.	Connected health systems can improve the quality of care to patients. Hence, health systems must have a unified design to achieve interoperability.	The analysis of data traffic, tracing of users, determining efficient routes for sending and receiving data can help determine the scalability of blockchain.

[51]	Healthcare System	Personal Health Data Sharing	Crypto tokens allow for the exchanging and selling of health data	Cloud technologies will provide off-chain storage for health data.	Security measures used to safeguard health data include encryption, public key management, and hash function.	Hash functions will provide data tracking, thus ensuring data integrity.	Functions of the proposed system include data quality, data sharing, cloud storage, data encryption, and crypto tokens.	Hence, a data-sharing system can be useful in managing large amounts of health data.
[52]	Healthcare System	Privacy and Authentication of EHR Data	Doctors can share EHR data by sending the address of the data through blockchain.	Data storage is in both on-chain and off-chain.	A decentralized attribute-based signature (DABS) will provide security such as unforgeability, collusion attacks, and anonymity	Digital signatures will provide data integrity by authenticating the identity of the sender and validates the data transferred.	Exchanging of EHR data must protect the identity of the patient.	Examining the network size and the potential number of threats can certify the scalability of the DABS system.
[53]	Healthcare System	Health Records and Information Management System	Blockchain can connect disparate healthcare systems into a single system by enabling peer to peer interoperability.	The user of the system stores its health data.	Blockchain provides security and tracking protocols for patient data.	The use of cryptography on the blockchain can control data accessibility by ensuring data privacy.	Costs associated with deployment and maintenance can contribute to the functionality of the blockchain system.	Further software development and system integration are significant for scalability.
[54]	Healthcare System	Healthcare Virtual Organization	Individuals can share health records in a virtual breeding environment (VBE) using blockchain for verification and validation.	A virtual organization facilitates communication and collaboration between patients and healthcare providers.	The use of cryptography enhances security on the blockchain.	Blockchain can protect the integrity of medical records through user verification and validation.	Blockchain can make healthcare services more accessible with less cost.	Blockchain is an emerging technology with lots of potential in being widespread among healthcare providers in the future.
[55]	Cybersecurity	Blockchain and IoT Security	Standardization of medical data is essential to facilitate interoperability.	Cloud data centers store all medical data.	Secure storage is a lacking component regarding digitally signed documents.	Data integrity is essential in the areas of data generation and data accessibility.	Blockchain can provide a standardization method for controlling access to medical data.	Blockchain can provide more security and scalability for increasing users given in a network.
[56]	Healthcare System	Blockchain and Smart Contracts	The interoperability of healthcare systems requires 1) Standardization of information flows, 2) Establishment of access rights, and 3) Creation of a patient identification system.	Reliable and safe storage of data is a requirement of an integrated electronic medical record (IEMC) system.	Cryptography provides the security of health information shared.	As data shared in the network is tamper-proof, this will ensure transparency to all users in the system.	Using blockchain can help modernize current healthcare practices.	Scalability needs improvement regarding large scale medical record sharing.
[57]	Healthcare System	Automated Remote Patient Monitoring	Applying blockchain technology to EHR will assist in providing interoperability in the healthcare industry.	Cloud computing and relational databases store EHR data.	Healthcare blockchain systems can be secure by being HIPAA compliant and by utilizing smart contracts control data transfers.	To create an accurate timeline, data records regarding the identity of the user and the treatment of a patient.	Designated nodes in the blockchain can execute smart contracts and verify new blocks.	More substantial corporations can build large scalable blockchain systems.
[58]	Healthcare System	Software Patterns in Blockchain-based Health Applications	Software engineering practices, including Abstract Factory, Flyweight, Proxy, and Publisher/Subscriber, can be used to address interoperability challenges.	Proper design considerations can reduce computer computation, minimize data storage requirements and overhead costs.	Balancing the integration of disparate systems with the security of health is still a concern. Security beyond encryption protocols of data is needed.	Data integrity can be difficult and costly to attain, seeing as each copy of the data must be reevaluated or recalculated.	The proposed system will provide a portal for patients to access health care services online.	Scalability remains an issue as a large number of patients, healthcare providers, and other users will be using the system.

[59]	Health and Privacy Regulations	Blockchain and Smart Contracts	Smart contracts assist in the sharing of medical data.	Consent for sensitive information and protected health information (PHI) is on the blockchain ledger.	Smart contracts and the Hyperledger Fabric system provide security of data.	A proof system specific to health data is critical to ensure the integrity of the blockchain system.	Permissioned networks will allow for a more straightforward application of consent management, data sharing and data collection.	Measuring the scalability of the blockchain will require increasing the number of nodes and data.
[60]	Medical Image Sharing	Blockchain and Smart Contracts	Medical images are shared through smart contracts directly with the use of a credit scoring system.	Users of the network require to have backup storage for data shared in the blockchain.	Blockchain will provide the security methods for cross-domain sharing of medical data.	Blockchain can provide integrity, given its trustworthy and reliable sharing database system.	The functionality of the blockchain system can be improved to provide efficient access to medical data.	Scalability is a concern due to the lack of format standardization for medical data collected by different healthcare institutions.
[61]	Multiple Approaches	Smart Contracts	Smart contracts provide interoperability, given its flexibility and adaptability with different systems.	Coding used for smart contracts is on the blockchain.	Improper execution of smart contracts can result from technical flaws in coding.	Data accessed through third-party applications reduces data integrity for users in the blockchain system.	Various blockchain platforms, such as Ethereum, can provide multiple functionalities and flexibilities.	Minimizing data stored on the blockchain will assist in improving scalability.
[62]	Healthcare System	Blockchain and Smart Contracts	Creating an online health data management system that allows individuals to share or sell health data for research purposes.	Health data will be stored locally on the patient device or a remote database server.	Key cryptography and digital signatures provide security mechanisms.	The proof-of-work mechanism which uses hash functions to validate new blocks of data reduces data forgery.	Blockchain can increase the quality of services by offering high-performance transaction rates.	A general readable health data format and having nodes to store data locally can assist in advancing the scalability of the system.
[63]	Healthcare System	Blockchain and Smart Contracts	Blockchain can consent to share patient medical information with doctors and pharmacies.	Plaintext prescriptions are stored using smart contracts. An Inter-Planetary-File-System (IPFS) will be used to store EMR data.	Security guidelines include damage control, modularity, and checks-effects.	Cryptography will provide integrity and confidentiality of medical information shared in the network.	Smart contracts can manage and trace communication among patients, doctors and pharmacies based on the proof-of-concept application.	Better speed, privacy, and scalability of the blockchain system are in a tradeoff of immutability and censorship.
[64]	Distributed Storage	Secret Sharing on the Blockchain	Private key encryption facilitates the sharing of data in the network.	A distributed storage mechanism will provide better data insurance in the blockchain	Private key encryption will allow for data to be confidential.	There is a substantial cost to validate a current hash value.	A peer network, along with a hash chain, is used to connect peers, clients, and orderers.	Storage remains a concern for the scalability of blockchain solutions.

Table 5 Comparative Analysis Table

Chapter 3: Problem Identification

In chapter 3, we identify the gap analysis in our research. We list down all the weaknesses in the existing approaches. Also, we present a problem statement that attempts to fill in the gaps found in the literature review. Lastly, we introduce our research objectives.

3.1 Gap Analysis

Based on the literature review performed in Chapter 2, a summary of the main gaps in the research is as follows:

- There is a limited amount of papers presenting a healthcare-based use-case model that focuses on the sharing of EMR data via blockchain.
- Protecting the patient's identity and ensuring the confidentiality of health data continues to be an essential area for research.
- Providing access management rights of patient data by ensuring the ability to access and restrict patient data is crucial to ensuring interoperability between hospitals and clinics.

3.1.1 Interoperability

The KONFIDO project [34], which is a system the provides health data exchange in Europe, is an innovative method to improve interoperation between patients and healthcare organizations. Presently in Canada, sharing medical data openly and publicly is uncommon due to the differing views of trust and privacy regarding medical data. Blockchain can also improve the data sharing of electronic health records (EHR). In contrast, data standardization is a significant gap in the exchanging and sharing of health

data within the blockchain network. Also, open standards of health data exchange are in development. A large number of users can create interoperability issues.

With the use of blockchain technology, patients and healthcare providers can be interconnected in a digital network through contracts that allow for sharing and exchanging of medical data. Potential healthcare applications that can be introduced include health data trading, an information hub for healthcare specialists and researchers, and an online prescription delivery service. Blockchain can provide better access to health data for health research. Additionally, establishing nationwide interoperability can provide safer and efficient data sharing. However, various regulations and cost-effectiveness must be examined. Also, blockchain can provide a network that can connect disparate health systems. Software engineering practices can assist in addressing interoperability challenges. Smart contracts open the possibilities for flexibility and adaptability between disparate systems.

3.1.2 Storage

Users of the blockchain network require technical skills to store and manage data. Storage systems must support integration between multiple systems. Current data stored in blockchain must meet minimum storage requirements and be interpretable universally. Computation performance, data storage requirements and storage costs can be improved. Storage optimization can reduce the amount of data stored and can allow for faster performance of the blockchain system. Cloud based-storage and relational databases will be used to store patient medical data and provide an off-chain/backup storage. As opposed to storing patient medical data on blocks, parts of the medical data such as metadata or anonymous data are stored on the blockchain.

Blockchain allows for the storing of data on different nodes in the network. Technologies such as edge computing can assist in the processing and storage of data on the blockchain. Seeing as multiple users will be storing data on various nodes in the blockchain, a proper storage management system is needed to process and manage data efficiently.

3.1.3 Security

The time and location of each transaction can be traced using blockchain technology. Data accessibility presents a concern as all information is immutable and copied to all nodes in the blockchain. Additionally, authentication and recovery of data can be improved. Given the use of smart contracts, improper execution of code can lead to security flaws.

Health data can be exchanged anonymously using blockchain technology. Current opportunities for blockchain technology include supporting existing health applications. The integration of health systems presents a concern to security given the sharing of health data.

3.1.4 Integrity

Verifying information stored on the blockchain can be costly. All blocks must be linked to the previous block. Hence, the larger the blockchain, the longer the time is needed to verify the existing blocks. In addition, previous data must be re-evaluated to ensure that data integrity is maintained. Data accessed through third parties reduces the integrity of the system.

Government regulations and consensus of users of the blockchain system assist in ensuring data integrity and privacy. Blockchain can provide a network for efficient

communication and collaboration between patients, doctors, and researchers. As a result, data consistency can be maintained as digital signatures can verify and authenticate data transfers. A proof system specific to health data will be useful to ensure data integrity.

3.1.5 Functionality

Multichain blockchain does not rely on proof-of-work mechanisms. Public health applications are costly and difficult to maintain. Permission requests received by patients via blockchain allow for efficient access to healthcare data for doctors and researchers. Blockchain can improve the accessibility of health data.

Smart contracts have the potential to store, update, and trace data between patients, doctors, and researchers in real-time. Also, smart contracts can increase the functionalities of blockchain. Other technologies can be used alongside blockchain technology. Functionalities of blockchain include processing transactional data and sharing data in peer-to-peer networks. Blockchain has the potential to provide benefits, reduce costs, and increase efficiency in the healthcare sector.

3.1.6 Scalability

Collaboration with government, researchers, health organizations and telecommunications companies is needed for scalability. Scalability can be improved by utilizing zero-knowledge proof through verifying the user's ability to perform the transaction without revealing information about the user and the amount of data they have. The capacity of transactions performed in the blockchain can be improved. Storage optimization remains an obstacle for scaling a blockchain system. Also, speed, latency, throughput, and network size of sharing data on a blockchain is a challenge given the processing of a large number of transactions. The integration of disparate systems can

improve scalability. Minimizing and standardizing data stored on the blockchain will improve the scalability of the system.

Proper analysis of scalability capabilities related to blockchain applications is needed. Blockchain can reduce the number of data intermediaries. Further research and development of e-health management systems are in demand. Analyzing data traffic will assist in determining efficient routes for sharing data. The scalability of the blockchain system can be tested by increasing the number of nodes and data.

3.2 Problem Statement and Research Objectives

After performing the literature review, proposed systems that provide interoperability, security, and scalability are limited. Based on the gap analysis performed in the previous section, existing approaches of accessing and sharing of medical data can be improved as well as new approaches that can be introduced given the use of blockchain technology.

In our research study, we aim to examine two critical topics about providing access to medical records electronically via blockchain technology. The first objective of our research is to provide smart access to patients' medical data. We aim to create a model that improves the accessibility of medical records by automating the process of sharing health data between patients, doctors and researchers. Smart contracts, which is an application or written code that executes terms of a contract, will be used in conjunction with blockchain technology to help coordinate health data found across various hospital institutions [16]. In addition, smart contracts will support the storing of health data in our blockchain system.

The second objective of our research is to improve the security features of our proposed solution by ensuring that users in our blockchain model can share medical data safely and confidentially. As mentioned in the literature review, one of the challenges associated with sharing health data electronically includes digital identity management. In order to prevent identity theft and forgery in our blockchain model, we implement a secret sharing scheme invented by Shamir [79] and Blakley [80] to provide secret access to medical data. Shamir's secret sharing scheme is combined with blockchain technology to support the sharing of patient medical data secretly by creating shares of the patient's digital identity. In doing so, Shamir's secret sharing scheme provides patients with a secure system that can verify, authenticate and protect the patient's identity when accessing health data electronically.

Chapter 4: Proposed Solution

In the context of the gap analysis and problem statement in the previous section, our approach involves using blockchain technology, smart contracts, and secret sharing for enhancing authorized access to medical data. Our proposed healthcare information system will introduce a new method for accessing, exchanging and sharing medical data efficiently and securely.

Blockchain technology brings a distributed and decentralized approach that is useful for providing authorized access to medical data. In our approach, blockchain will verify the identities of patients and healthcare providers. Throughout the patient life, blockchain can accurately record health data ensuring authenticity given the tamper-proof feature in the blockchain. For instance, patients often visit various health organizations for different needs. A patient can visit a hospital for a surgical operation, an eye clinic for an eye exam or a dentistry clinic for teeth cleaning. Hence, blockchain technology can be used to record and validate patient interactions through the consensus of doctors, health insurance organizations, and government agencies. Once an interaction is validated, given the consensus of most users in the blockchain network, the interaction is then recorded in the blockchain.

The use of smart contracts in our approach will provide an efficient way to track and store health data across various hospital institutions and users in the blockchain. Smart contracts allow for better security of health data. Thus, ensuring that health data cannot be changed or lost without the permission of the data owner. In addition, using smart contracts will improve the flexibility of our system. Smart contracts provide an automation solution

that can store transactions into relevant blocks. With limited dependence on an intermediary or third-party, the speed of transactions stored on the blockchain increases.

Secret sharing can preserve privacy standards for health data. In our approach, the public keys of users will be secretly shared and split into multiple parts. As a result, to reveal the public key of a user in our blockchain system, many shares will need to be collected and combined to reveal the user's identity. Therefore, secret sharing provides an alternative to single key sharing and reduces the risk of data loss and identity theft by not allowing hackers to steal public keys.

4.1 Overall Conceptual Architecture and Design

The outline of the proposed blockchain system, as shown in Figure 4, begins with setting the government as the central system administrator. The purpose of setting the government as the central authority is to pre-screen the healthcare institutions and patients participating in the network. Also, the government's role is to put patients first by protecting their identities from hackers and adversaries. However, setting the government as the central authority does not translate to a centralized organization making the decisions. Additionally, the validating of blocks in our proposed solution will be a decentralized process resulting in receiving a consensus from many nodes in the network. Most importantly, the role of the government is to monitor the blockchain system by safeguarding the privacy and confidentiality of sharing EMR data. As a result, the government will be in a better position to regulate, restrict, and control the network by maintaining the access and permissions of data shared between healthcare institutions and patients.

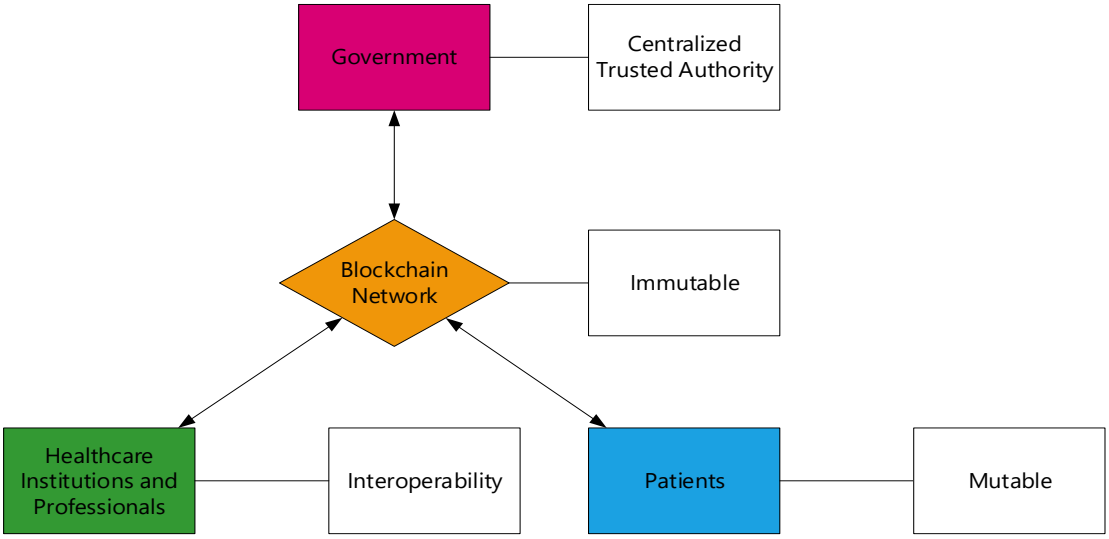


Figure 4 High-level design of Blockchain-based Healthcare Solution

Moreover, the proposed conceptual architecture involves providing enhanced authorized access to EMR data secretly among many entities within a single network. In doing so, building trust among several entities is crucial in order to facilitate efficient access to EMR data. The proposed conceptual architecture, as shown in Figure 5, is a hybrid permissioned system solution that has the functionalities of both public and private blockchains. Thus, the proposed consortium blockchain allows certain entities to read, verify, and access transactions. Based on the various entities in the blockchain system, each entity will have a specific set of permissions to perform certain tasks based on their identity and roles in the system. The administration of permissions is determined based on the user application.

In our consortium blockchain network, miners will maintain the shared ledger by validating transactions without being able to read the data. As a result, data transfers between entities will be unhackable. Hence, miners can validate blocks without having to read them. Additionally, verified entities, as determined by the system administrator, can participate in the blockchain network. In addition, the system administrator will be used to

override, edit or delete entities that are maintaining the shared ledger. Also, the entities in the proposed architecture are pre-validated due to preserving the authenticity of the network. Other entities including patients, private clinics, pharmacies, laboratories, physiotherapy, dentistry, require multiple authentications checks.

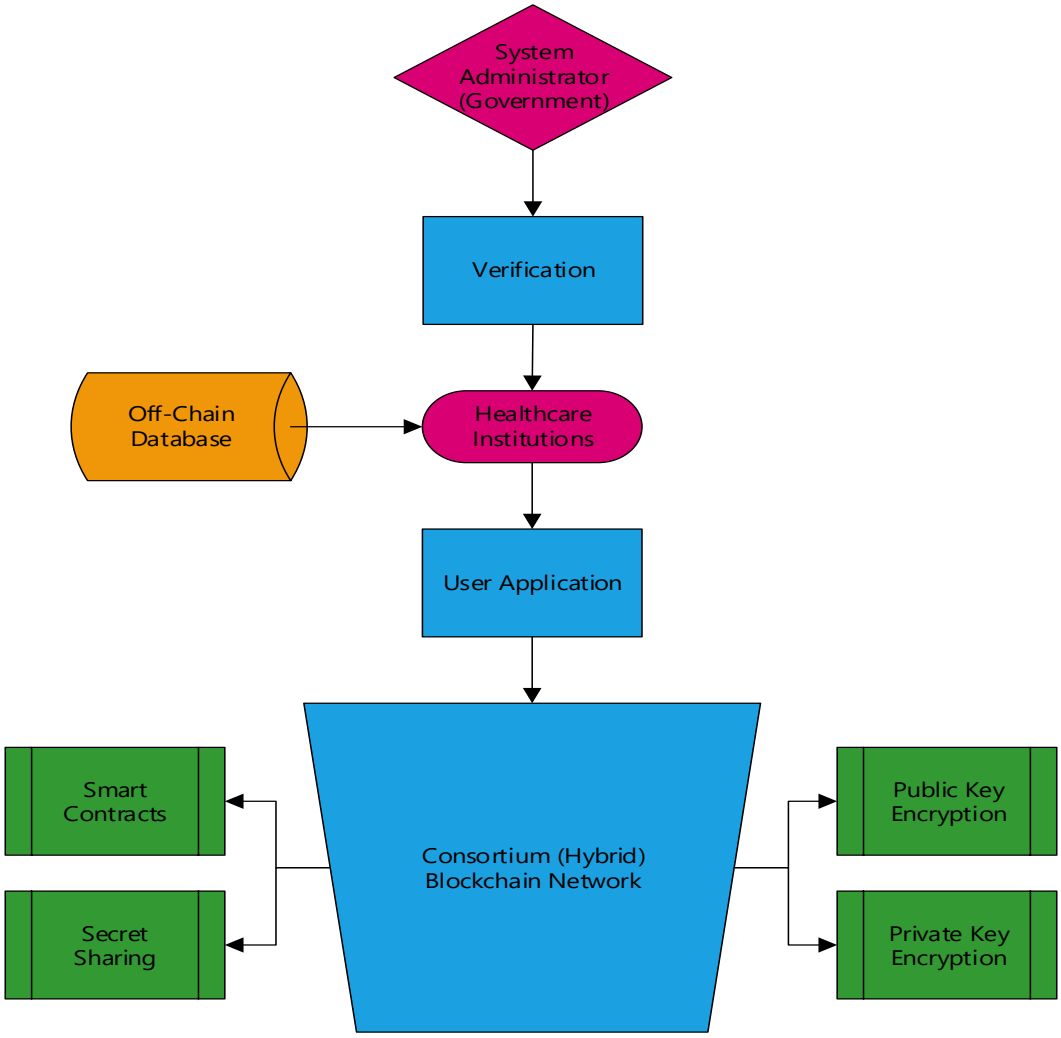


Figure 5 Conceptual Architecture

Currently, medical data is stored in the databases of hospitals and clinics. Additionally, medical data can be stored in various formats including a print-out, a patient-clinic portal, an email, and a cloud-storage. As a result, storing medical data in various locations reduces the access shareability of patient medical information. Given the

scattered amount of information across different systems can potentially reduce the quality of information. Blockchain can reduce the gap between various data formats by establishing new ways to connect various systems which will, in turn, allow information to be shared and accessed efficiently.

Furthermore, EMR's will contain a series of health information collected by health institutions, including hospitals, clinics, and pharmacies. Metadata will then be taken from the EMR's and stored in a block. As a result, the blockchain network will connect EMR data from all hospitals, clinics, and pharmacies into a single system. Hence, the metadata stored in the blocks will verify and validate the identity of a patient. Also, the metadata will provide access to medical data to users of the network based on the access permissions in place. Once a user's identity is verified and permissions are granted via blockchain, patients will be able to connect to various health institutions to access and share medical data electronically.

Each block will contain a series of information detailing the transfer of data in the blockchain network. Currently, given the average storage size of a block which is usually limited to 1 megabyte (MB) and the average time required to create a block which is 10 minutes, storing copies of patient medical data on the blockchain is insufficient. In addition, given the immutability of blockchain technology, storing data on the blockchain system can present security concerns as information on the blockchain cannot be deleted or altered.

The most common structure of a block includes the block number, the data, the nonce value, the block hash value, and the previous block hash value. Additionally, the block structure involves using hash functions performed using cryptography. Thus,

cryptographic hash functions allow data in the blocks to convert to a series of letters and numbers that hide the data stored in blocks. The most common type of hash function used in the blockchain is called SHA-256, which stands for Secure Hash Algorithm 256 bit. It is important to note that each hash value is unique given its association with the data. As a result, each block data cannot have the same hash value. Also, if the data in the block is changed, then a new hash value must be generated.

Entities	Attributes
• **Patients (P)**	• Identification #, Name, Address, Phone, Age, Gender, Weight, Date of Birth, Health Card #, Social Insurance #, Medical History (diagnosis, medications, and lab and test results)
• **General Practitioner (GP)**	• Identification #, Name, Position, Department
• **Physician Specialists (S)**	• Name, Location, Role,
• **Laboratory Technicians (LT)**	• Name, Location, Role,
• **Pharmacists (PS)**	• Name, Location, Role,
• **Hospitals/Clinics (HC)**	• Identification #, Name, Address, Phone
• **Medical Laboratory (ML)**	• Identification #, Name, Address, Phone
• **Pharmacy (PH)**	• Identification #, Name, Address, Phone

Table 6 Attributes for Entities/Actors in the Healthcare System

To better explain the process of sharing medical data on the blockchain, table 6 presents a list of identified entities and links of all possible actors. In the proposed architecture, each entity has roles and permissions based on their unique identity description and list of attributes. Entities in the presented in the use-case diagram include patient, hospital/clinic, pharmacy, and medical laboratory.

Additionally, figure 6 presents a use-case diagram involving the interactions between patients and healthcare institutions, as well as what data is being shared and exchanged. As shown in figure 6, each entity has a relationship with one or more entities types. In each relationship, data or information exchanges occur between each entity. For instance, a pharmacy has multiple relationships including the patient, hospital/clinic and

medical laboratory. The pharmacy also shares and exchanges information such as a patient medical record between a medical laboratory and hospital/clinic. Therefore, every entity is interconnected while remaining independent from each other.

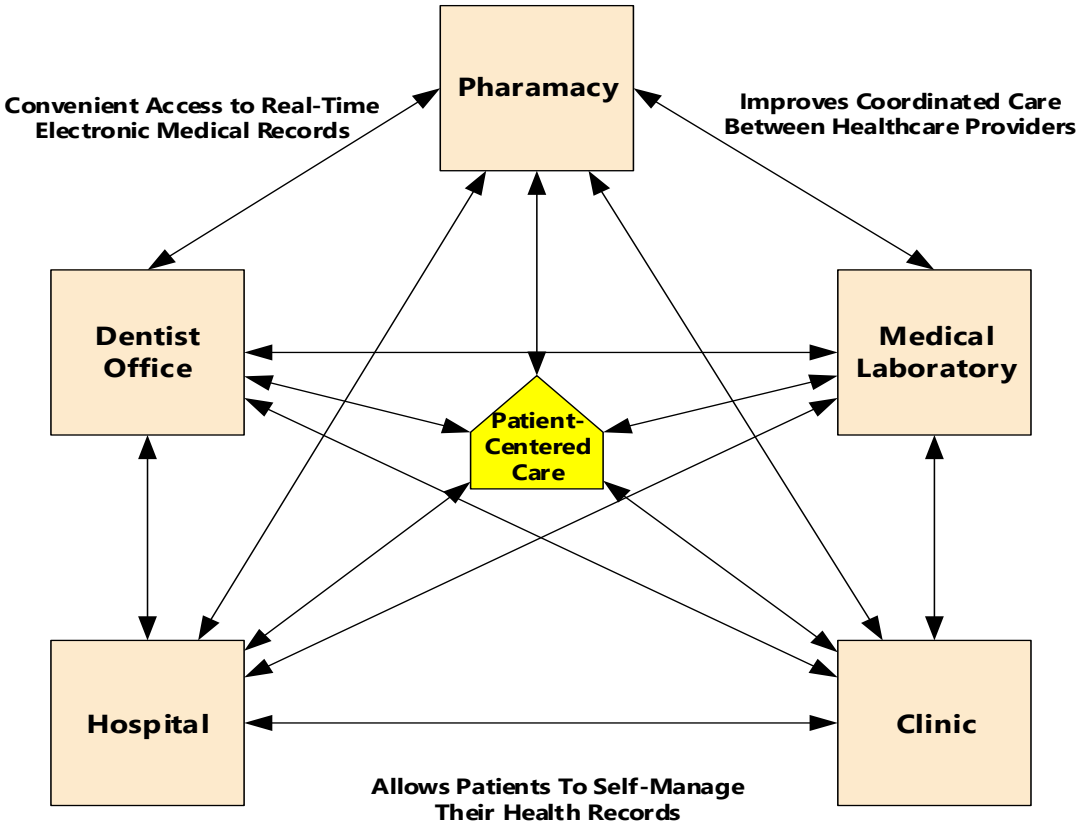


Figure 6 A Use-Case Diagram for collaboration between Healthcare Institutions and Patients

The proposed use-case diagram design is patient-centric. Hence, patients will be controlling how their medical data is accessed and shared through blockchain. In addition, providing patients with the opportunity to share and access their medical data digitally can improve the quality of health services. In doing so, blockchain can provide patients with the transparency needed to allow effective sharing of their medical data. Additionally, patients can communicate with doctors and hospitals regarding their medical status with the use of a public key management system. On the other hand, with the use of smart contracts, patients can restrict access to their medical data. Thus, smart contracts set the

standards and conditions based on the preferences of patients. For instance, patients can digitally choose to give or revoke access to their medical data to a doctor, a family member, or an insurance company.

4.2 Detailed Technical Architecture

The detail technical design of our healthcare blockchain model represents a data workflow of storing patient medical data via blockchain. In addition, health data must follow a specific data structure validated by smart contracts. Data exchanged and shared will also be supported by Shamir's secret sharing algorithm. The primary users of our proposed system include the patient, the healthcare provider, and the health researcher.

4.2.1 Off-Blockchain Layer

As presented in the detailed technical architecture in Figure 7, the designated health data extracted from a health database. The health database stores information such as EHR's of patients including personal information, medical records, and payment transactions. It is essential to recognize that all the information found in the health database is not stored on the blockchain. Only the EMR metadata of the patient is stored on the blockchain. After extracted, the health data is sent to the smart contract to be processed.

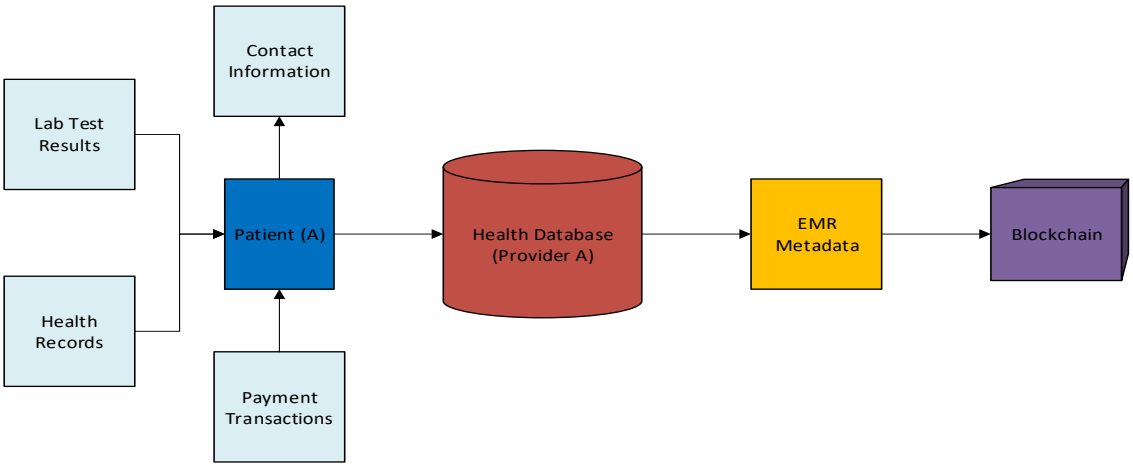


Figure 7 Storing EMR Metadata in Blockchain

4.2.2 Smart Contract Layer

In the smart contract level, smart contracts are created based on the specifications given by the users of our blockchain. Users can create smart contracts that control the storage process of their data in the blockchain. In the smart contract, the user will describe the conditions for a transaction to be verified. For instance, a provider may request the name, date of birth, and health number to provide patient access to their health data. As shown in Figure 8, once the smart contract verifies the transaction, it will be added to the blockchain. In addition, the purpose of having smart contracts in our blockchain is to automate the process of storing access permissions to health data. When a transaction occurs, the smart contract will manage the information by reducing the costs and computational consumption of storing the transaction in the blockchain.

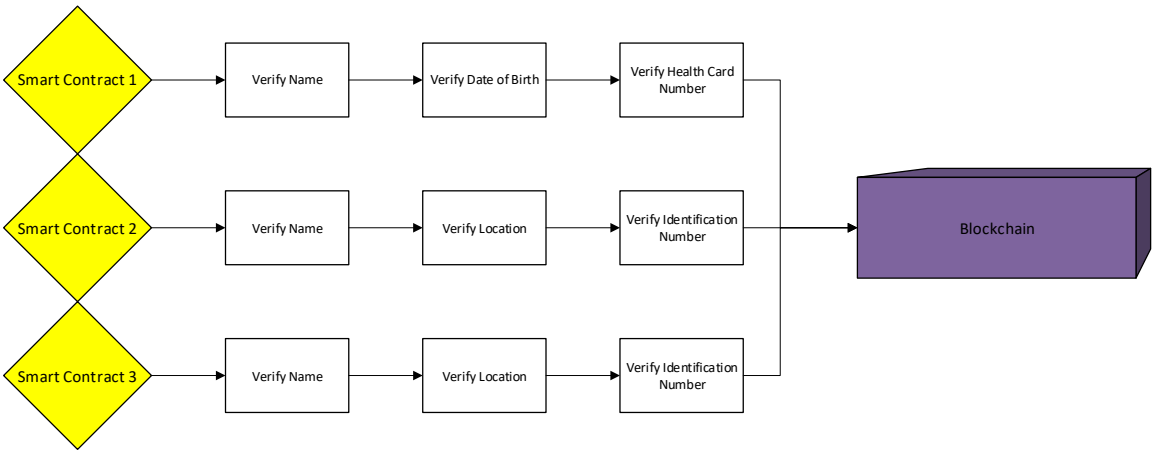


Figure 8 Smart Contract Process

4.2.3 On-Blockchain Layer

As presented in Figure 9, all transactions must be verified before being broadcast to all the nodes in our blockchain network. Transactions will be validated through the consensus of verified miners, which, in turn, reduces the vulnerability of security attacks in our blockchain. In addition, to recover a transaction stored on the blockchain,

information provided by the smart contract will be used to verify the identities of users in the network. If the user's identities are verified, the smart contract will relocate the block containing access to the medical data requested by the user.

In the event of tampering of transactions, a copy of the current hash function of each block will be stored in the healthcare database as a point of reference. As a result, the hashing algorithm found in our blockchain, as discussed in the algorithm design section below, can be used to calculate the hash function of the block and compare it with the hash function stored in the healthcare database. If the hashes do not match up, it is evident that the data has tampered. Hence, changes in the hash function of a block can be seen, which, in turn, helps maintain the integrity of our blockchain model.

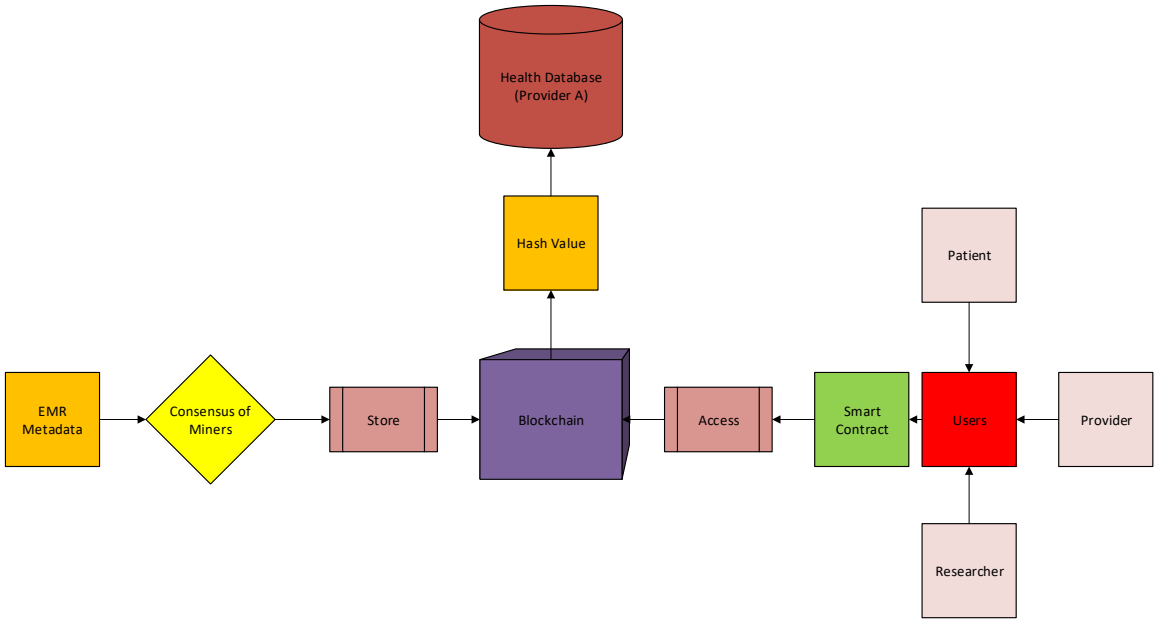


Figure 9 Storing and Accessing EMR Metadata on Blockchain

4.2.4 Privacy Layer

As shown in Figure 10, each user in our blockchain model has both a public and private key. It is most common in blockchain applications that the public key of users is widely shared among other users in the network [11]. However, the distribution of public

keys in our model will be limited to ensure confidentiality and to protect our users' identities from forgery and fraud. The user's public key will be split into multiple shares, thus, improving the security standards in our blockchain model. Also, each share of the user's public key will be distributed based on the user's request. Hence, a threshold number of shares is needed to uncover the public key. As a result, the transaction associated with the public key can be retrieved from the blockchain.

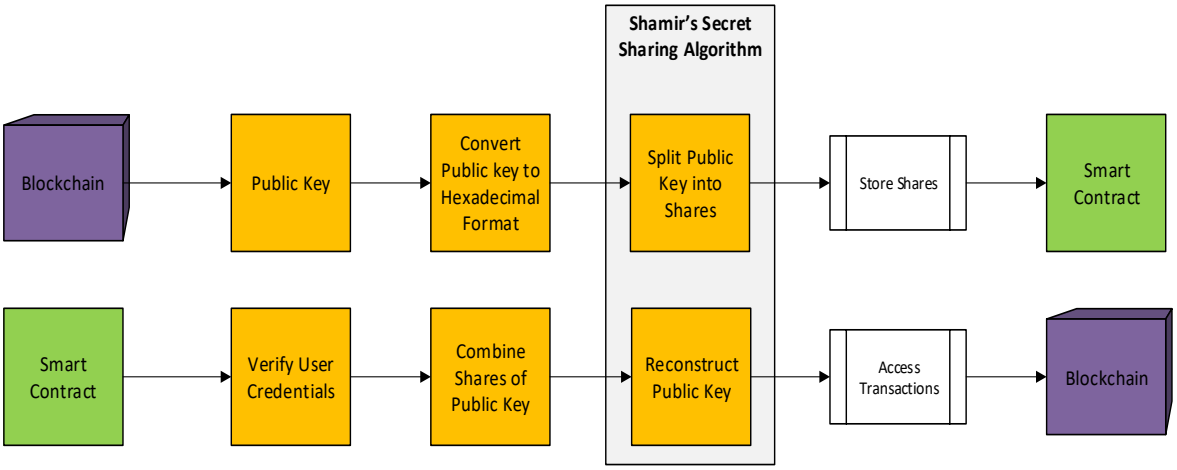


Figure 10 Encrypting and Decrypting of Public Keys Using Shamir's Secret Sharing

4.2.5 User Layer

As shown in Figure 11, users can access health data depending on the specifications of the smart contract. To retrieve a transaction stored in our blockchain, a user must have the public key of the data owner. Thus, the user must obtain shares of the data owner's public key. Shares of the public key are created using Shamir's Secret Sharing Scheme [79]. Once the shares of the public key are retrieved, the user can reconstruct the shares using Shamir's secret sharing scheme to reveal the public key. Subsequently, the user can search for the transaction on the blockchain by using the public key of the data owner. Lastly, the private key of the user is used to decrypt the transaction.

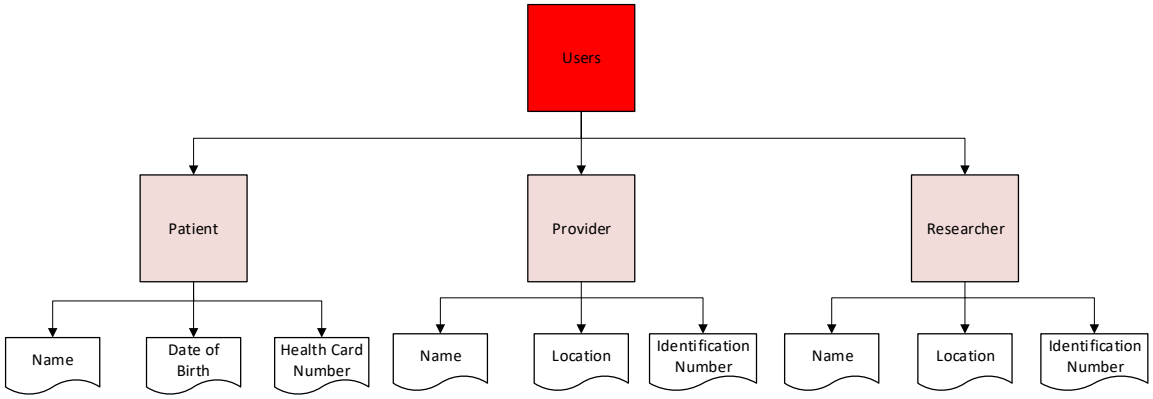


Figure 11 Users in our Healthcare Blockchain Model

4.3 Design Discussion

As presented in Figure 12, our proposed healthcare blockchain model is designed to be a cost-efficient solution for patients, doctors, and medical institutions for addressing accessibility and interoperability concerns of medical records and data. The three main reasons for designing our model is to maximize the interoperability, security, and functionality capabilities of EMR data.

Overall, the use of blockchain technology can have patients access their medical data at any time without having to go through a medical institution. Likewise, health data found in databases across hospitals and clinics can utilize blockchain technology to store accessibility permissions. Traditionally, the transferring of health data is performed through the reliance of a centralized system. In contrast, our blockchain offers an alternative approach by providing a distributed storage system to store accessibility permissions. Thus, patients and doctors with permissions can access authorized medical data. With the use of blockchain as a distributed system, health data can be exchanged among different hospitals, which, in turn, shows the interoperability of our healthcare blockchain model.

Combining Shamir's secret sharing [79] with blockchain technology is a unique approach to improving the security standards in our healthcare model. Our use of secret sharing allows for medical data to be shared secretly by safeguarding that the digital identity of users. In our model, secret sharing gives a patient the ability to access their medical records on demand. Secret sharing also allows a patient's medical data to be shared with other users in the network. For instance, if a patient needs immediate medical attention, an ambulance can gain authorized access to the patient's medical data through obtaining shares of the patient data through blockchain. Therefore, by distributing several access shares of a patient's medical data in the blockchain network, each user with a threshold or a higher number of shares can gain access to the patient medical data.

Moreover, the use of smart contracts in our healthcare model provides better support for verifying transactions on the blockchain and managing the users of the network without the need for an intermediary. Using smart contracts ensures that agreements and conditions between users are imposed and executed without the risk of fraud or contract breaches. As a result, smart contracts improve the functionality of our healthcare model by reducing the time and resources needed to authorize and share medical records.

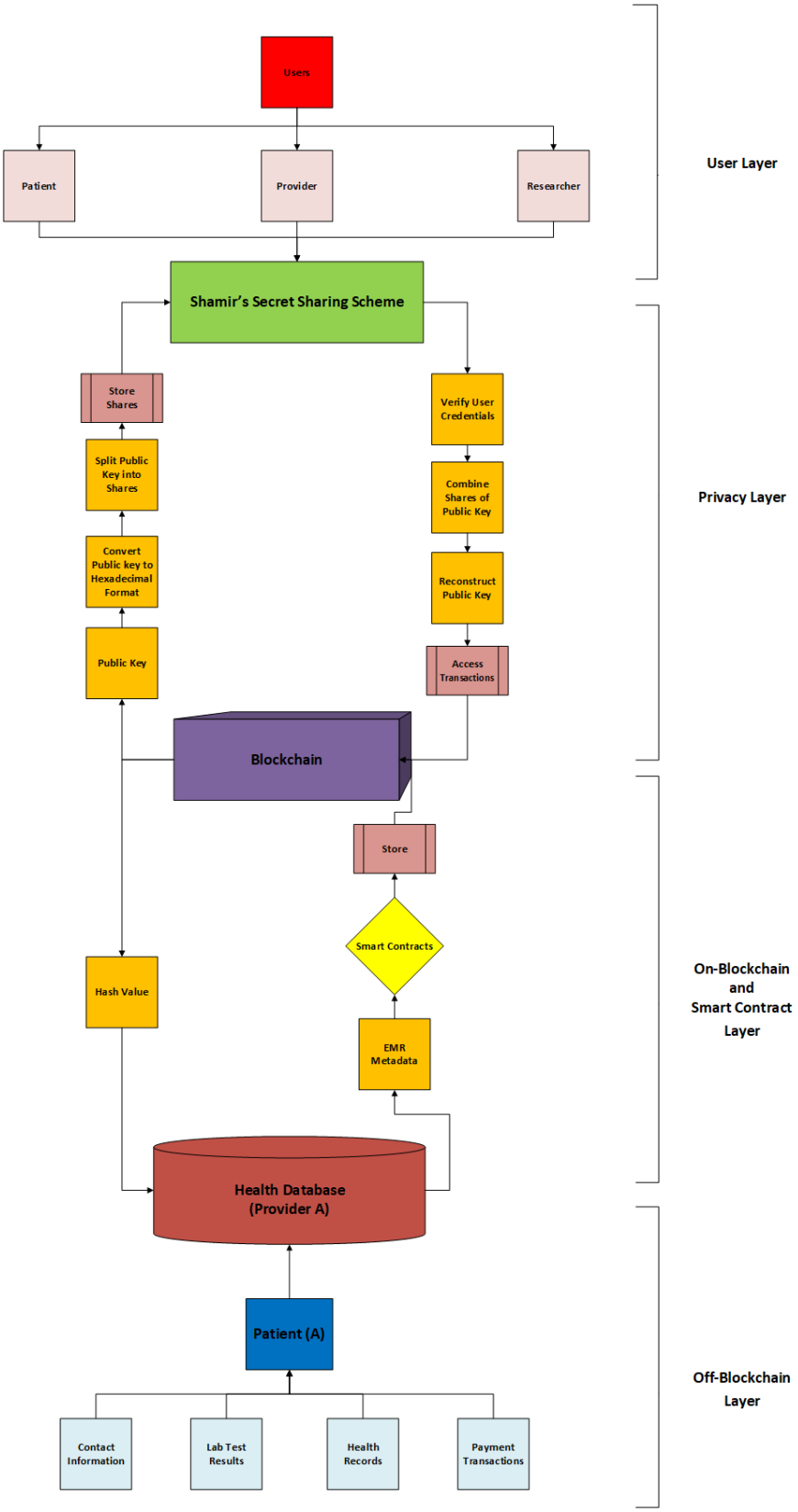


Figure 12 Overall Integrated Architecture

4.3.1 Alternative Design Considerations

Relatively, several design options can support better accessibility to EMR's. In this section, there are three alternative approaches to our healthcare model which will include the use of various database sharing technologies. It is crucial to understand each alternative presented is a feasible solution to enabling efficient accessing and sharing of electronic medical data. However, each alternative may also not be the optimal solution available.

An alternative to using blockchain technology is to store EMR data on a single centralized relational database. All medical data of patients will be stored and uploaded on a single shared database that can be accessed by all hospitals in the network. An advantage of using a centralized system includes reducing redundancy of data being copied across many nodes. Additionally, implementing a centralized database system can lead to increasing interoperability as medical institutions can jointly connect to the same database. A disadvantage of using a centralized database involves a high risk of medical data being stolen or lost. In addition, having many users such as patients and hospitals using a centralized database presents a concern for network traffic which can result in congestion when connecting to the database.

Similarly, another alternative to blockchain technology is adopting a cloud storage service for storing electronic medical data. Cloud storage significantly provides an improvement from a centralized database design in terms of handling large volumes of data as well as a large number of users. An advantage of using cloud storage includes higher reliability of accessing data promptly because of faster processes performed by multiple data centers. With the use of high-speed networks, cloud storage offers the option for increasing data storage capacity while maintaining speed and reliability. Thus, cloud

storage provides a feasible solution to improving scalability by accommodating increases of users and data in the network. In contrast, a drawback of cloud technology involves the security and compliance risks. Essentially, the storage of sensitive medical records of patients via cloud servers is a significant risk as data is in possession of a third-party supplier.

Comparatively, design options that are direct alternatives to blockchain technology include the use of distributed ledger technologies. Examples of distributed ledger technologies consist of Hashgraph, Directed Acyclic Graphs (DAG), and Holochain [72]. As presented in Table 7, each technology listed varies in its application regarding mining and validation of transactions. The advantages of distributed ledger technologies regarding the handling of electronic medical data are dependent on the consensus algorithm and approach to validate transactions. For instance, Hashgraph mines transactions through a virtual voting system whereas a public blockchain uses a proof-of-work mechanism through rewarding miners with crypto tokens [72].

In the same way, the disadvantages of using distributed ledger technologies include that they are costly to maintain. Thus, the larger the blockchain, the longer the time is needed to verify the existing blocks. Therefore, in order to ensure the data integrity of the chain, previous blocks of data must be re-calculated.

Distributed Ledger Technologies	Mining of Transactions	Validation of Transactions
• **Hashgraph**	• Virtual voting	• Depends on the consensus algorithm
• **DAG**	• Reliant on validation of previous transactions	
• **Holochain**	• No need for mining or validation as each node processes its ledgers.	

Table 7 Examples of Distributed Ledger Technologies (DLT)

4.3.2 Reasons for Design

The design in our proposed solution is unique in comparison to other health blockchain systems. Firstly, our systems provide additional security measures to ensuring the privacy of sharing patient information. Transactions can be sent and received in our system by gaining access to the public key. Therefore, gaining access to one's public requires obtaining a minimum threshold value of shares. Using Shamir's secret sharing, users can reveal the public key which is needed to send or receive a message in the network. As a result, each node in the network can validate transactions from a user by decrypting the message after obtaining the public key.

Another novel feature in our proposed system is the use of smart contracts with health records. Hence, smart contracts provide a better verification and tracing of transactions performed in the network. All transactions sent are processed, logged and posted on the relevant block in the blockchain. In addition, our choice of using blockchain technology in oppose to other digital ledger technologies because it is the most popular digital ledger technology to date. Currently, there are more than 50 real-life use cases of health blockchain systems [73]. Hence, with a considerable amount of research and applications of health systems using blockchain, this provides an immense opportunity to compare our proposed solution with real-life use cases.

4.4 Algorithm Design (Pseudocode)

Our proposed solution reflects a proof-of-concept representation of a real-life health blockchain system. Based on the idea of blockchain technology supporting existing healthcare applications, our goal is to deliver accessible EMR's to patients efficiently and cost-effectively.

So far, in our proposed solution, we were able to understand the process of building a health-based blockchain system. In this section, our next step is to determine whether a potential relationship can exist between blockchain and electronic medical records. Lastly, our final step would be implementing our algorithms by developing a simulation through coding.

Algorithm 1 The blockchain model

```
function requirements of the block
    Set timestamp as a parameter
    Set previous hash function as a parameter
    Set current hash function as a parameter
    Set block data as a parameter
    Set the digital signature as a parameter
end function
function creating a new block
    Calculate the timestamp of the block
    Calculate the previous hash function by using the current hash function from the previous block
    Calculate the digital signature of the block by using the user's private key and converting it to a hash function
    for the current hash function
        create a hash from the data
        calculate the hash value using the SHA-256 algorithm
        return hash of the data as the current hash function
    end for
    return the timestamp, previous hash function, current hash function, data, and digital signature for the newly mined block
end function
function building of blockchain
    Set the first block as the genesis block in the blockchain
    Add a new block using the function mining of the block
end function
```

The first algorithm, see algorithm one below, explains the rules and requirements of our health blockchain model. The first function in our algorithm introduces the data structure found in a block. Each block in our blockchain must contain the following

parameters which include a timestamp, a hash function of the previous block (excluding the genesis block), a hash function of the current block, data that is to be stored on the blockchain, and a digital signature. It is essential to realize that more parameters exist in comparison to a block used in the application for Bitcoin. Hence, our choice of using the listed parameters provides a more explicit way of presenting our understating of blockchain. The second function in algorithm 1 describes the process of creating a block. To explain, when a block is created, the function calculates the timestamp which is used to ordering the blocks. Next, the hash function of the current block is calculated by converting the block data into a hash using the SHA-256 algorithm. Subsequently, the digital signature found in the block is calculated by converting the public key of the user into a hash using the SHA-256 algorithm. The third function in our algorithm explains the process of building our blockchain. Therefore, the first block of our blockchain is called the genesis block which will result in all blocks can be traced.

The second algorithm, see algorithm two, examines the implementation of Shamir's Secret Sharing algorithm in our health blockchain model. The first function of establishing the secret message is by converting the public key of 'u' user to a hexadecimal format. The second function splits the secret message into 'n' number of shares. Next, this function also sets 't' as a threshold that will prompt the reconstructing of the public key. It is important to remember that $n \geq t$. The third function describes the steps for reconstructing the public key. Using the Lagrange Basis Polynomials formula, the public key is reconstructed by combining any t-out-of-n parts. The last step would be to revert the hexadecimal to reveal the public key.

The third algorithm, see algorithm three, uses smart contract technology to manage the security and accessibility of electronic medical records between a patient, a health organization and a health researcher. The smart contract will ensure that all rules and conditions are executed and maintained. In addition, our smart contract will implement protocols to secure information exchange that is obtained by authorized users.

Algorithm 2 Implementation of Shamir's Secret Sharing Scheme of a Public Key

```
1:  function creating the public key as a secret
2:      Set public key of the user as the secret
3:      for the public key
4:          Convert public key to hexadecimal format
5:      end for
6:     Print the hexadecimal format of the secret
7:  end function
8:  function splitting secret into shares
9:      for the secret split into 'n' number of shares
10:         Split secret into 'n' number of shares, using Shamir's Secret Sharing algorithm
11:     end for
12:     for 't' is the threshold
13:         Set 't' as a threshold for revealing the secret
14:         Set 't' as less than equal to 'n'
15:     end for
16: end function
17: function combine shares into the secret
18:     if the secret is to be reconstructed
19:         then 't' out 'n' shares is required
20:         combine shares into secret
21:     else if then 'n' out of 'n' shares is required
22:         combine shares into the secret
23:     else if the secret cannot be reconstructed
24:          Print error message
25:     end if
26:     Convert hexadecimal secret to reveal the public key
27: end function
```

The smart contract presented in algorithm three follows a data sharing approach in dealing with managing electronic medical records. The first function in our algorithm assigns parameters based on the identity of the user. For instance, if the user is a patient, then our system will request information such as the patient name, date of birth, and health card number. The second function in the algorithm verifies the user's input with the data requirements in the smart contract. If the user's input data is verified, then the smart contract stores the user's data in the blockchain.

Algorithm 3 Smart contract terms and conditions for health data storage

```
function define users and conditions of contract
if the user is a patient
        Set patient name as a parameter
        Set patient date of birth as a parameter
        Set patient health card number as a parameter
        Set response of terms and conditions as a parameter
    else if the user is a health individual/provider/organization
        Set name as a parameter
        Set location as a parameter
        Set the identification number as a parameter
        Set response of terms and conditions as a parameter
    else if the user is a health researcher individual/provider/organization
        Set name as a parameter
        Set location as a parameter
        Set the identification number as a parameter
        Set response of terms and conditions as a parameter
    else
      print error message
    end if
end function
function verify user's input data using smart contract
if the user's input data match format data stored in the smart contract
       Create a block of user's data using algorithm 1
    else
      print error message
    end if
```

4.5 Implementation details and Action Planning

The main aim of our proposed solution is to provide accessibility of health records in a secure, interoperable, and efficient way. The use of blockchain technology, Shamir's secret sharing scheme and smart contracts will be assessed in comparison to current practices of sharing health records.

In our implementation of the proposed solution, a proof of concept approach is presented in order to evaluate the effectiveness of sharing health records in a distributed environment. The proof of concept application consists of three levels: storage of transactions on the blockchain, encrypting and decrypting of public keys using Shamir's secret sharing, and establishing data storage via smart contracts.

Furthermore, to demonstrate the capabilities of our proposed solution, we build a simulation of a potential use-case involving sharing electronic medical records. Firstly, transactions created by patient, provider and researcher users' will be stored in the blockchain. Secondly, Shamir's secret sharing scheme will be used to split the user's public key into multiple shares. These shares will then need to be reconstructed in order to reveal the user's public key. Lastly, smart contracts will be used to provide more functionality of the blockchain system relating to the automation of storing transactions in the block.

In the proposed blockchain system, doctors will be able to search and access patient data. The patient must first provide proof of identity to be able to share and access their medical data. Transactions posted on the blockchain will validate the patient's identity and will give the patient access to their medical data. Sample data that the patient must provide in order to prove their identity include name, date of birth, and healthcare number.

Each transaction recorded in the blockchain must first be verified by validating patient information through a trusted authority (i.e. the government). Correctly, in the blockchain system, smart contracts will be used to process the patient data to determine the identity of the patient. Once the identity is confirmed, the transaction will then be posted on the blockchain which will then be validated by miners in the blockchain network.

In our example, a coded application will be presented to describe the process of the patient receiving access to their medical data. In this code, various steps in the verification and accessibility of health data will be shown. The code provided is not a fully functioning blockchain application. However, our code determines the feasibility of the proposed solution and evaluates the concepts discussed in this paper.

This implementation of our blockchain solution borrows heavily from Krunal blockchain in JavaScript code [74]. The code of Krunal was used to build our blockchain simulation. Additional codes were written, which, in turn, extend the original codes built by Krunal. The implementation of Shamir's secret sharing code implementation coded was taken from secrets.js-grempe. The original code was created by amper5and [75].

Chapter 5: Evaluation

In this chapter, we evaluate our proposed solution based on four features: functional, complexity, efficiency, and comparative analysis. We also provide discussion and implications about our proposed solution.

5.1 Functional Analysis

In the functional analysis section, we perform system tests on our blockchain model, smart contract protocol, and secret sharing scheme.

5.1.1 Blockchain System Testing

The block class in our code provides an outline for the creation of new blocks. The parameters of each new block in our blockchain is as follows: each block must contain a timestamp, last hash function of the current and previous block, and a digital signature. Each parameter in the block has significance as it will provide information about the accuracy and integrity of the blockchain.

```
const GENESIS_BLOCK = {
    timestamp: Date.now(),
    lastHash: ' ',
    hash: '4733596e89a7ebfd4d390e857e3658b67bf1f8f98940f77923028d7f8e233113',
    dsign: '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff',
    data: 'John Smith,10/10/1990,19426789510'
};

// publickey: 'MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAecQSkSyGKIr/hMwnCnZSICJty1c/'
// privatekey: 'MIIBOgIBAAJAecQSkSyGKIr/hMwnCnZSICJty1c/nBhyQv92uLZoll9jOG3NkHSFIwV62yo6PdNbLndzim'

module.exports = { GENESIS_BLOCK };
```

Figure 13 Input Code of the Genesis Block

The genesis block or block 0 represents the first block in our digital ledger. As shown in figure 13, the data coded in the genesis block is inputted manually before running the code. Calculating the hash function of the genesis block, and the digital signature was completed using an online hash generator was used [76].

The purpose of the timestamp is to provide a reference for when a block was added to the blockchain. The timestamp determines which miner validated a block first. Seeing the timestamp is tamper-proof, the sender cannot alter the timestamp. Therefore, the timestamp offers a precise measurement for the mining of the block.

Additionally, the current hash function of each block is calculated based on the data inputted in the block. The hashing of the data is performed using the SHA-256 algorithm which converts the data into a string containing numbers and letters. Converting the data using a hash function improves the security of the blockchain as the output of the hash function is unidentifiable given its length and format. In addition, hashing a block requires large amounts of computational power. Each block in the blockchain, excluding the genesis block, must contain the hash function of the previous block. Hence, if the data on the current block is changed or deleted, this will result in the hash function of the current and previous blocks to be recalculated. Consequently, once data is added to the blockchain, it is incredibly challenging to alter the data as large amounts of computer power is needed to recalculate the hashes of the previous blocks.

The digital signature used in our blockchain model is calculated by converting the public key of the user to a cryptographic hash. Instead of using the user's public key to record transactions on the blockchain, we utilize a digital signature to provide authentication of the block without revealing the user's identity.

```
Blockchain {
  chain:
   [ Block {
       timestamp: 1575141520123,
       lastHash: ' ',
       hash:
        '4733596e89a7ebfd4d390e857e3658b67bf1f8f98940f77923028d7f8e233113',
       data: 'John Smith,10/10/1990,19426789510',
       dsign:
        '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
```

Figure 14 Output of Genesis Block Code

The output of the genesis block, as shown in Figure 14, displays the results of the timestamp, current hash function, data and digital signature. The actual results of the output of the code match our expected results. To further explain the output of the code, the timestamp returns a UTC represented in milliseconds, the current hash function is calculated by converting the data input into a hash value. Lastly, the digital signature is calculated by converting the private key into a hash value.

```
static mineBlock({lastBlock, data}) {
    const timestamp = Date.now();
    const lastHash = lastBlock.hash;
    const dsign = lastBlock.dsign
    return new this({
        timestamp,
        lastHash,
        data,
        dsign,
        hash: cryptoHash(timestamp, lastHash, data)
    });
}

   addBlock({ data }) {
       const newBlock = Block.mineBlock({
           lastBlock: this.chain[this.chain.length-1],
           data

       });

       this.chain.push(newBlock);
   }
```

Figure 15 Code for Adding the Block

After adding the genesis block and the hash function to our blockchain, we then create a function to generate new blocks. As displayed in Figure 15, the mining of the block includes inputting the data and hash function of the previous block.

```
Blockchain {
  chain:
   [ Block {
       timestamp: 1575141520123,
       lastHash: ' ',
       hash:
        '4733596e89a7ebfd4d390e857e3658b67bf1f8f98940f77923028d7f8e233113',
       data: 'John Smith,10/10/1990,19426789510',
       dsign:
        '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
     Block {
       timestamp: 1575141520132,
       lastHash:
        '4733596e89a7ebfd4d390e857e3658b67bf1f8f98940f77923028d7f8e233113',
       hash:
        'a0dd1b2af5ec12f9e70992f1740060a0492227d7b48a162c6ddcb97c7ddf631c',
       data: 'Terry Williams, 05/05/1995, 15412368740',
       dsign:
        '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
```

Figure 16 Output for Adding Block code

As shown in Figure 16, the output of the code returns the timestamp of the new block, the previous block hash function, the new block hash function, the data and the digital signature.

5.1.2 Smart Contract Testing

Moreover, in our blockchain, we have added a smart contract feature to automate the adding of data to our blockchain. To execute the smart contract, we first get the block data and then parse it by extracting each field of the data. Each data sent to the smart contract must follow the format requirements before entered in the blockchain. Using the split method function in JavaScript, we can create an array of substrings by splitting the data. Using a nested if statement, we check if each substring follows the format of the smart contract.

Test Summary	Input Steps	Test Specifications	Test Data
Smart Contract 1: Patient data	User must provide smart contract #, name, dob, health id	(SC1, Name, dd/dd/dddd, ##########)	(SC1, Tim Juniour,02/23/1990,12456987156)
Smart Contract 2: Provider data	User must provide smart contract # name, location, and id	(SC2, Name, City, #####)	(SC2, Jessica Hollins, Halifax,14597)
Smart Contract 3: Researcher data	User must provide smart contract # name, location, and id	(SC3, Name, City, #####)	(SC3, Harry West,Toronto,16516)

Table 8 Test Case Summary for Smart Contract

Using a black-box testing technique, we evaluate the functionality of our blockchain model by performing a test case on our smart contract algorithm. A summary of our test case is presented in Table 8. In our smart contract algorithm, we have three smart contracts. The first smart contract (SC1) involves processing patient data. The test specifications for each field in SC1 includes 'name' as only letters (A-Z, a-z), 'date of birth' following a date format (dd/dd/dddd), and 'health id' as only numbers and containing precisely 12 digits. Additionally, the data format for the second smart contract (SC2) and the third smart contract (SC3) is the same. The test specifications for each field in SC2 and SC3 includes 'name' as only letters (A-Z, a-z), 'location' as only letters (A-Z, a-z), and 'health id' as only numbers and containing precisely five digits. As shown in Figure 17, if the smart contract approves the data entered, then the data is entered in the blockchain.

```
Block {
  timestamp: 1575141520137,
  lastHash:
   '95fb6de1b21cc5ad2898ac5678dc6991ef84eecbf01a37f0e87760a7cefdff4f',
  hash:
   '0745e5fd979fcf8ff0425a056b442fe04b91a9ccc93d2c26c157183e29e56580',
  data: 'SC1,Tim Juniour,02/23/1990,12456987156',
  dsign:
   '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
```

Figure 17 SC1 Output Code

Furthermore, an equivalence test is performed to assess the functionality of our algorithm further. In our analysis, incorrect data will be inputted into the smart contract. Both the expected and actual output will be compared in order to determine the reliability of our algorithm.

	Test Case #1	Test Case #2
Equivalence Testing	Approve data entry equal to SC1, SC2, or SC3	Approve patient data health id containing numbers equal to 12 digits
Expected Results	The algorithm will deny input data not equal to SC1, SC2, or SC3	The algorithm will accept input data equal to 12 digits
Actual Results	Pass, the smart contract behaves as expected	Pass, the smart contract behaves as expected

Table 9 Actual and Expected Results

As shown in Table 9, the results of the equivalence testing prove that in test case #1, the smart contract algorithm allows data entries that contain only SC1, SC2 or SC3. Therefore, entering non-existing smart contracts will result in the system denying incorrect data entries.

Additionally, in test case #2, the inputted health id of a patient must be equal to 12 digits. The results indicate that data incorrectly entered, including data that are less than or more than 12 digits, is denied by the algorithm. Thus, the smart contract algorithm behaves as expected.

5.1.3 Shamir's Secret Sharing Testing

Furthermore, the use of Shamir's secret sharing [79] improves the security of our blockchain model by restricting access to the public key. Shamir's secret sharing requires obtaining a threshold number of shares to uncover a user's public key. For instance, in Figure 18, the public key of Patient A is split into four shares with a threshold of two

shares. Therefore, in order to get permission to access to Patient A's health data stored on the blockchain, a user must receive at least two shares of Patient A's public key.

```
PS C:\Users\Abdihakim Mao\Desktop\HealthBlock Code> node sshare.js
MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAecQSkSyGKIr/hMwnCnZSICJty1c/
show all shares:
801ed8ab4af46d033020d3fac0ad502a1230741a762628c729cdd354c40b4f21ed2fc930df5d0b5426dba6a391abf86088c3fd9fcd0465a4860d80ce
48de512c05a67aa1c5651a15ad1278728260c4b82fa838ec45a546788154994bfd154c4eb110643e1c017212909918d229a34239078706b46f42efd2
1b860d72258cc0ca576
802c70975438cbd66071a0f45b1b7575fcd0e1e531ac4c0e4fea79f986e754b3c7ce5891a6ebda0846269a572a263ca10d87e66e5368c41907dadedd
5f4d7819d1bce8a3872a2c6b4494e8a508f183f191c1bcd9577a83d0dec92f36370a866cbe10c54df382ed852aa3fdc44c768f73d2de0088c1e5c144
2a1c02a442585d2573b
8032a83c1ecca6d5504171fe9d86264fe97092bf432a60f962b7af9d474c1d722ed197417ec6d58c667d3e04bcadc05181f41f8199fca48d87675b23
12832f05d24a961246ef310eeca697a78e814139bb59807516cfc0b85bbdb25dce4fcf320b10a593e9b398f7bcbae1866075cbbad1e9029cab372b86
35da08a660e4998f200
8049312ea860567cc0d346f8ada73fdbe0c1ca0a6ea9558d53a53d62d32ea24783dd7bd3445678a157cd226e4cfc6522070fc05d7e705773d474732b
706b3ba279981ca703a590875649c90a0c030d732cd364b372d4d891a03393dc62f4d3f8b1c187aa3d55c37a4f17e7e887dd0427a87ddce05d7b8db8
4939dcd88df1773aea1
combine 2 shares:
802c70975438cbd66071a0f45b1b7575fcd0e1e531ac4c0e4fea79f986e754b3c7ce5891a6ebda0846269a572a263ca10d87e66e5368c41907dadedd
5f4d7819d1bce8a3872a2c6b4494e8a508f183f191c1bcd9577a83d0dec92f36370a866cbe10c54df382ed852aa3fdc44c768f73d2de0088c1e5c144
2a1c02a442585d2573b
8032a83c1ecca6d5504171fe9d86264fe97092bf432a60f962b7af9d474c1d722ed197417ec6d58c667d3e04bcadc05181f41f8199fca48d87675b23
12832f05d24a961246ef310eeca697a78e814139bb59807516cfc0b85bbdb25dce4fcf320b10a593e9b398f7bcbae1866075cbbad1e9029cab372b86
35da08a660e4998f200
MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAecQSkSyGKIr/hMwnCnZSICJty1c/
true
```

Figure 18 Secret Share of Patient A's Public Key

5.2 Complexity Analysis

According to algorithm 1, as discussed in the proposed solution section, the time complexity for when a block is added to the blockchain is linear and represented by O(n) where n is the number of blocks created. As users can store more than one transaction in a block, the number of steps required to add a block is dependent on the number of transactions included in the block. Creating a new block requires the calculation of the timestamp, previous hash function, current hash function, and the digital signature. In this step, the time complexity is constant at O(1). When adding the block to the blockchain, depending on the number of blocks created, the time complexity for adding a block is linear O(n). The overall complexity of algorithm one is represented as O(n).

In algorithm two, converting the user's public key into a hexadecimal format is a constant at O(1) as the time it takes for the secret sharing algorithm to make the conversion takes a single step. Next, splitting the public key into shares is dependent on the number of shares the user chooses. Thus, the time complexity for the user to select 'n' number of shares is linear at O(n). Finally, to reconstruct the public key, the combining of the shares represents $O(\log_n)$ because the algorithm may reexamine certain shares when determining if the user has the required threshold number of shares. Once the user's shares are examined, the algorithm reconstructs the shares to reveal the public key. The overall complexity for algorithm two is represented as $O(n) + O(log_n) = O(n\, log_n)$.

In algorithm three, the first step is to determine among the three smart contracts in our model is requested based on the data input supplied by the user (i.e., patient, provider, researcher). Seeing as there are two different data format requirements, the time complexity is linear O(n). Hence, if the user matches the data format outlined in the smart contract, then the data is then stored as a transaction in the blockchain. The time complexity for storing the data on the blockchain is linear O(n). The overall complexity for algorithm three is represented as O(n).

5.3 Efficiency Analysis

For evaluating the efficiency of our blockchain code, the analysis performed was completed in an Intel® Core™ i5-6200U CPU @ 2.30 GHz, 4.00 GB RAM, and Windows 10 Pro (64-bit operating system). Our blockchain code was written and tested in the Visual Studio Code and built using JavaScript programming language. We implement our blockchain model to include smart contracts and Shamir's secret sharing scheme.

Figure 19 represents a bar chart that shows the memory usage output for our blockchain code and smart contract algorithm. The chart is divided based on the number of data entries. In our model, four inputs consist of 10, 20, 40, and 100 entries. The output of the chart displays the memory used to process the code. Both the average heap used to execute the blockchain code and the smart contract algorithm independently is 4.34 MB.

As shown in Figure 20, the average resident set size (rss), which is the memory held in RAM for processing, is used to execute the blockchain code is 20.10 MB and the average rss used to execute the smart contract algorithm is 20.28 MB. The total heap provided is 9.73 MB. The output of the memory usage explains that storing data on the blockchain is relatively active.

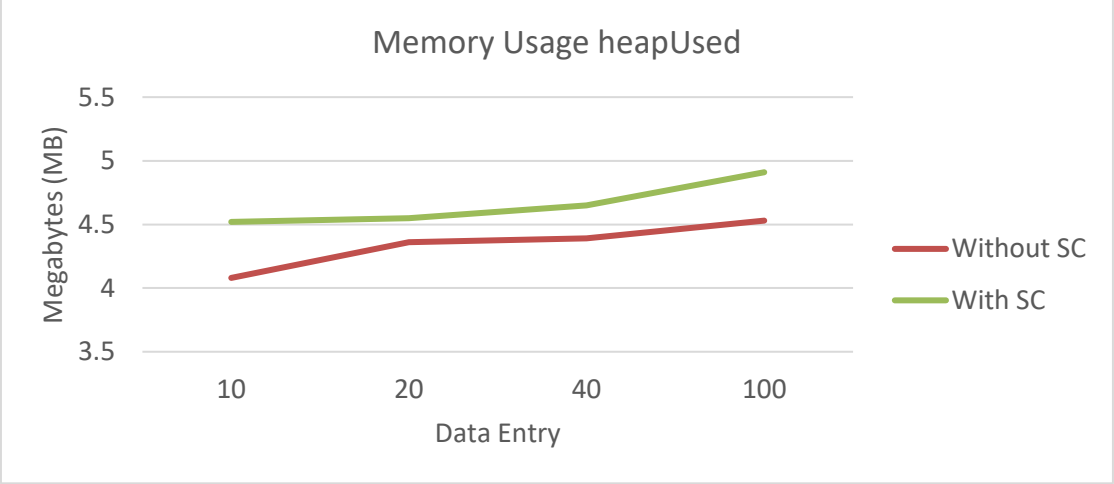


Figure 19 Heap Usage in The Blockchain Code and Smart Contract (SC) Algorithm Per Data Entry

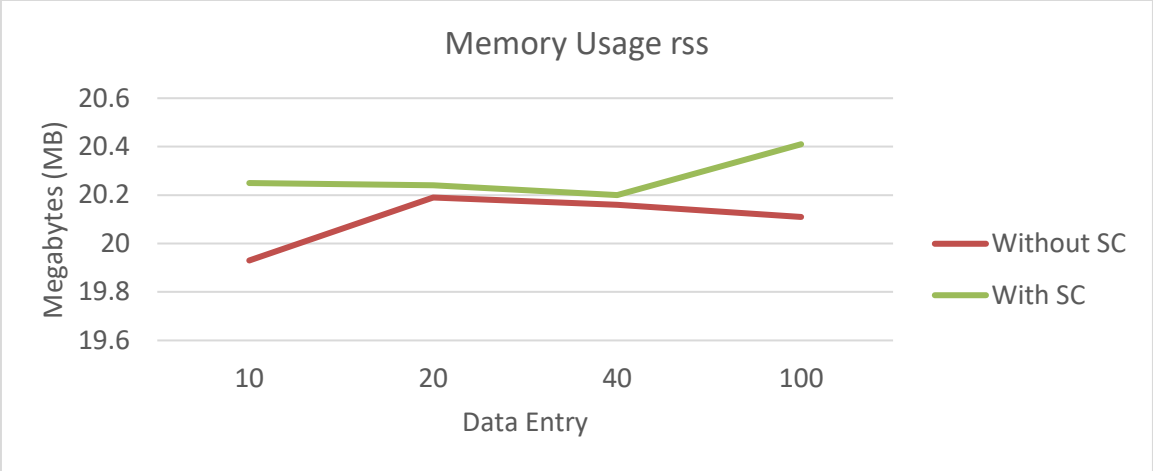
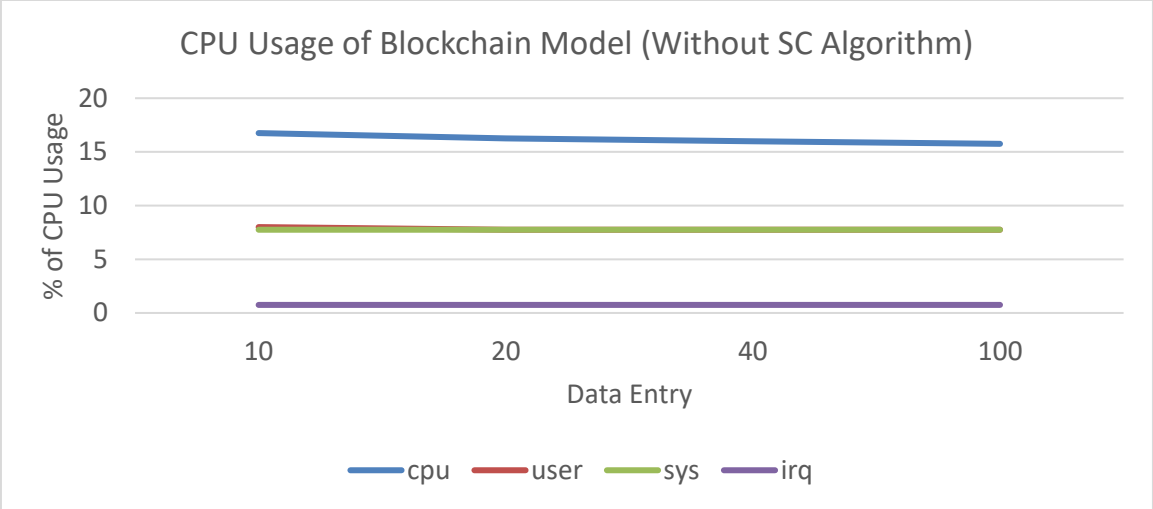


Figure 20 RSS Usage in The Blockchain Code and Smart Contract Algorithm Per Data Entry



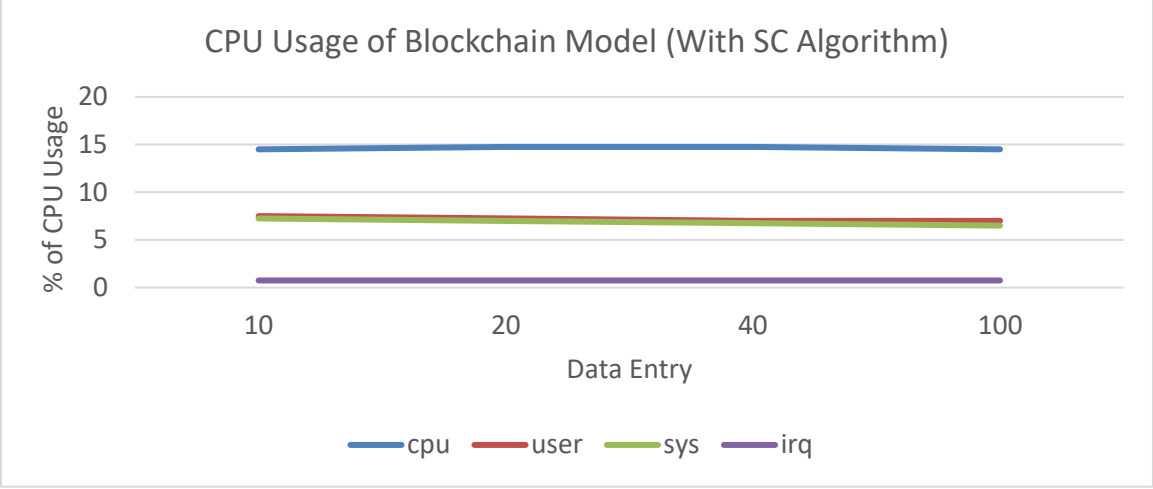


Figure 21 CPU Usage of The Sum of the Blockchain code and sum of the Smart Contract Per Data Entry

Figure 21 displays the sum of the CPU usage calculated for the blockchain code and smart contract algorithm. The type of computer consumption modes calculated includes the user mode, the CPU mode, the system mode and the IRQ mode. The colour in the bar chart illustrates details about the blockchain code and smart contract algorithm. The results of our code indicate that the smart contract algorithm executes a bit faster than the blockchain code. Thus, it can be implied that the smart contract algorithm improves our blockchain efficiency.

	Memory Usage	**CPU Usage**			
heapUsed	5.05 MB	-	-	-	-
rss	20.55 MB	-	-	-	-
cpu	-	17%	13%	15%	13%
sys	-	8%	6%	8%	7%
user	-	7%	6%	7%	5%
irq	-	2%	1%	0%	0%

Table 10 Memory and CPU Usage of Both the Blockchain Code and Smart Contract Algorithm

In table 10 displays the memory and CPU usage of our blockchain code and smart contract algorithm put together. The output of the chart shows that our proposed blockchain model can handle small amounts of data.

5.4 Comparative Analysis

In our comparative analysis, we will be comparing our proposed solution against four papers. The first two papers examined will be on health-based blockchain models that focus on managing the accessibility of healthcare data. Table 11 presents a comparative analysis of the blockchain-based papers. The remaining two papers will be about secret sharing schemes with a focus on hash functions.

Paper	MedChain	MedRec 1.0	Our Proposed Solution
Overall Architecture	• Hospitals servers will provide data sharing exchange • Metadata, including the location of health data, is stored off-chain	• MedRec utilizes blockchain technology and smart contracts in EMR • MedRec focusses on the patient and provider relationship	• Provide authorized access to medical data via blockchain technology • Track and store health data with the use of smart contracts • Preserve privacy standards for health data using secret sharing
Design	• Data sharing between hospitals and patients	• MedRec integrates blockchain technology with EMR infrastructure	• Our model provides the secret sharing of public keys and smart storage of EMR data on the blockchain
Key Features Offered	• Centralized authority to validate public keys	• Ethereum Smart Contract Model. • Mining of Blocks	• Smart contracts for automating data storage • Secret sharing of public keys of users
Size of Blockchain and Data	• 30 Blockchain Nodes • 10 Directory Nodes • 400 events in Block	• A prototype of MedRec has yet to be implemented	• 1 Blockchain Node. • Data tests performed on 10, 20, 40, and 100 records
Efficiency (Time Taken, Memory Usage)	• Efficiency depends on network connectivity • Network Latency average of 50 milliseconds	• A prototype of MedRec has yet to be implemented	• Storage of data records on the blockchain is relatively fast
Scalability	• Medchain model is scalable to an extent	• MedRec has the potential to support hundreds of providers	• Our proposed solution is scalable to an extent

Table 11 Comparison Analysis of Medchain, MedRec 1.0 and Our Proposed Solution

The overall architecture for the MedChain [41] model manages the access rights of medical data shared between patients and providers using blockchain technology. User identities in MedChain are certified using a central authority. Also, users can access their health data stored in a hospital or clinic server by getting verified through the blockchain. The design of the system includes data generation, session-based data sharing and key-management. Notable features found in MedChain include metadata update, storage space recycling and data stream support. The overall size of the MedChain blockchain includes 10 tasks completed in the directory node, 30 tasks completed in the blockchain node, and with each block size with a limit of a maximum of 400 events. Additional details about the MedChain model include the network latency being around 50 milliseconds and the scalability of the system remaining dependent on the number of users in the network. Lastly, MedChain paper [41] represents a feasible implementation in comparison to our proposed solution. MedChain provides a theoretical approach in modernizing healthcare information exchange by including various technologies such as IoT devices, mobile application support and blockchain technology.

Furthermore, MedRec's [42] overall architecture utilizes smart contracts to extract the metadata from a patient’s health data record. MedRec implements three smart contracts relating to a registrar contract, a patient-provider relationship (PPR) contract and a summary contract. MedRec also provides cryptocurrencies as a reward to users that validate transactions stored in the blockchain. Currently, the development of a MedRec prototype remains a work in progress. Therefore, information regarding the scalability, efficiency and complexity of MedRec has yet to be determined. Overall, MedRec [42]

provides a practical approach to implementing an accessible and flexible system using blockchain technology.

As shown in table 12, our proposed solution better manages public keys than MedChain [41] and MedRec [42] by creating and distributing multiple shares of a public key using Shamir's secret sharing scheme. Thus, distributing shares provides a more secure approach as opposed to sharing a public key openly. The goal of our proposed solution is to ensure data integrity and confidentiality by restricting the number of users with access to medical records in our blockchain network.

Characteristics	MedChain	MedRec 1.0	Our Proposed Solution
Permission Restrictions	• Permissioned	• Permissioned	• Permissioned
Consensus	• BFT-SMART and proof-of-stake protocol	• Proof-of-work protocol	• Our system is suited to a proof-of-authority protocol
Blockchain Structure	• Private peer to peer blockchain network	• Private peer to peer blockchain network	• Hybrid blockchain network
Security	• Use of a trusted authority for validating public keys	• Proof of work algorithm	• Centralized authority to validate user identities • Secret sharing scheme to protect ownership of the public key of users
Mining of Blocks	• Hospitals and supernodes can only mine blocks in the network	• Blocks are mined based on the Ethereum model	• Blocks are mined by trusted and selected nodes in the network

Table 12 Similarities and Differences Between Medchain, MedRec 1.0 and Our Proposed Solution

Moreover, the paper written by Chum et al. [77] further examines the efficiency of a hash function based secret sharing scheme approach. The paper published by Chum et al. [77] compares various hash-based schemes with Shamir's secret sharing scheme. The results of the study determine that the hash-based approached proposed six times faster than Shamir's secret sharing. Also, the paper shows that the hash-based sharing scheme is more efficient than Shamir's secret sharing.

In contrast to Chum et al. paper [77], the speed of executing Shamir's secret sharing algorithm in our proposed solution is marginal in comparison to the CPU and memory performance in our blockchain algorithm. Our decision to implement Shamir's secret sharing scheme is independent of the speed and performance of the secret sharing algorithm.

In addition, it is critical to acknowledge that Shamir's secret sharing scheme is the first form of secret sharing scheme invented to split and reconstruct a secret. Shamir's secret sharing can provide a secure and innovative system for sharing medical records between healthcare users such as doctors, patients, and researchers. As a result, secret sharing allows multiple users to store a duplicate copy of medical records in their local server. For instance, given the occurrence of a distressing event that results in a hospital's medical database server to crash, the medical database can be recovered by combining data parts stored in multiple shared databases found across nodes in the network. Hence with the application of Shamir's secret sharing scheme, medical records can be recovered and accessed by combining a threshold of parts. Therefore, Shamir's secret sharing scheme approach developed over 40 years ago, in turn, provides a more verified approach to implementing the sharing of medical data secretly and securely.

The study by Kalyan Alapati [78] uses a group-oriented approach to distribute shares of a secret using Shamir's secret sharing. The shares are then distributed by a dealer and given to a group of users. When reconstructing the secret, the dealer collects the shares from the group and converts the shares into the secret using Shamir's secret sharing. As a result, this method of sharing a secret is efficient for a group-oriented login.

In comparing the Kalyan Alapati approach [78] to our proposed solution, using a group-oriented approach can improve the accessibility of health data by sharing medical records of a patient among a group of healthcare professionals. Additionally, this paper [78] was chosen as a comparison as it provides an alternate approach to implementing Shamir's secret sharing by focusing on increasing the security and efficiency of data sharing.

5.5 Summary and Discussion

In the evaluation section, we have examined the functional, efficiency, complexity and comparison analysis with existing work. In table 13, we summarize the main findings from our evaluation. The following are the criteria for the evaluation section include interoperability, storage, security, integrity, functionality, and scalability.

Criteria	Our Proposed Solution
• **Interoperability**	• Metadata taken from health records can simply be inputted and shared in our blockchain
• **Storage**	• Data is easily stored on the blockchain given the use of smart contracts
• **Security**	• Applying Shamir's secret sharing strengthens the level of security in our blockchain by protecting the ownership of the public key
• **Integrity**	• Using a centralized authority allows for information to be easily verified on the blockchain
• **Functionality**	• Results of the algorithm tests performed optimally
• **Scalability**	• Our simulation can be scalable to accommodate many users.

Table 13 Summary of Evaluation Criteria of Our Proposed Solution

Based on our evaluation section, we have proved that blockchain technology can prevent and reduce inaccurate data. In our model, data is inputted and verified by the health provider. As a result, each data stored is highly accurate and correct based on the protocols embedded in our blockchain. Additionally, the use of smart contracts and Shamir's secret sharing scheme has dramatically enhanced the capabilities of our proposed model. Smart contracts can store, update, and trace data between patients, doctors, and researchers accurately. To improve data quality, we utilize smart contracts in addition to nodes to validate transactions by ensuring data entered in our blockchain meets the conditions for data integrity. On the other hand, Shamir's secret sharing was able to increase the security measures in our blockchain system. Using a secret sharing scheme safeguards public keys in our system to prevent users' identities from being falsified or compromised.

5.6 Limitations and Implications

In our study, there were several limitations regarding the implementation of our health-based blockchain model. Firstly, it was difficult to obtain a real-life primary care dataset containing the health information of patients. Our research study could benefit more from using accurate patient data to better understand the pros and cons of health data sharing in the blockchain.

Secondly, in the field of public health research, our study can improve substantially with the support of health institutions and relevant agencies. Conducting an internal analysis in conjunction with a hospital or clinic can help us gather better insights to develop a system to address concerns regarding the accessibility of medical data.

Lastly, our research was limited based on the high costs of deploying our model in a real blockchain environment such as Ethereum. Lastly, measuring the scalability of our

proposed solution was difficult due to not having several users participating in our network. Despite the limitation of measuring scalability, we were able to propose a feasible solution that can be tested and developed to perform in an actual blockchain setting.

Chapter 6: Conclusion

It is essential to understand that blockchain will not replace all technology out there. Currently, in the Canadian healthcare industry, medical data is stored electronically in hospital databases. As we have shown in our proposed solution, our research aims to make medical records more accessible electronically by connecting patients and healthcare institutions. Using blockchain technology, we were able to create a patient-centric use-case by providing patients with the transparency of medical records, convenience access, and coordination between hospital institutions, thus improving the quality of health services. Based on our experimental results, our decentralized approach for storing medical records was able to perform optimally. In comparison to our related work, our study was able to expand in critical areas including interoperability, security and functionality.

In addition to accessibility, another major takeaway from our research involves enhancing the security and privacy standards of medical data shared electronically. With Shamir's secret sharing scheme in combination with smart contracts, patients can manage their medical records efficiently and safely. The use of smart contracts in our proposed solution automates the verifying of transactions in our network. Also, secret sharing ensures that patients' digital identities are protected when accessing medical records.

Overall, based on what our research suggests, we believe that blockchain can improve the accessibility of health data. We also believe that blockchain has the potential to provide benefits, reduce costs, and increase efficiency in the healthcare sector in Canada. We hope that our proposed health-based blockchain system will be useful to improve the patient experience with hospital services and provide a collection of medical data that can be shared safely and securely.

Chapter 7: Future Work

Using blockchain technology requires proper infrastructures to manage various stakeholders in the system. However, a lack of resources can impact the building of the desired blockchain infrastructure. Blockchain-based solutions are better when tailored to solve a specific issue as opposed to being based strictly on existing applications such as Bitcoin. Also, understanding the infrastructure will assist in determining what data to store or not store on the blockchain.

Furthermore, examining the features and efficiency levels of current health systems will assist in proposing insightful research and implementing better solutions. Public health applications are costly and difficult to maintain. Introducing human-centric approaches to increase accessibility can increase the scalability levels of a blockchain system. Therefore, providing easy access to health records can save time and costs for both patients and health institutions.

Appendices

Appendix A

Application of JavaScript Code (Inputs)

genesis.js > ...

```
const GENESIS_BLOCK = {
    timestamp: Date.now(),
    lastHash: ' ',
    hash: '4733596e89a7ebfd4d390e857e3658b67bf1f8f98940f77923028d7f8e233113',
    dsign: '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff',
    data: 'John Smith,10/10/1990,19426789510'
};

// publickey: 'MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAecQSkSyGKIr/hMwnCnZSICJty1c/'
// privatekey: 'MIIBOgIBAAJAecQSkSyGKIr/hMwnCnZSICJty1c/nBhyQv92uLZol19jOG3NkHSFIwV62yo6PdNbLndzim'

module.exports = { GENESIS_BLOCK };
```

block.js > ...

```
const { GENESIS_BLOCK } = require('./genesis.js');
const cryptoHash = require('./crypto-hash');

class Block {
    constructor({timestamp, lastHash, hash, data, dsign}) {
        this.timestamp = timestamp;
        this.lastHash = lastHash;
        this.hash = hash;
        this.data = data;
        this.dsign = dsign;
    }

    static genesis() {
        return new this(GENESIS_BLOCK);
    }

    static mineBlock({lastBlock, data}) {
        const timestamp = Date.now();
        const lastHash = lastBlock.hash;
        const dsign = lastBlock.dsign
        return new this({
            timestamp,
            lastHash,
            data,
            dsign,
            hash: cryptoHash(timestamp, lastHash, data)
        });
    }
}

module.exports = Block;
```

JS crypto-hash.js > ...

```
const crypto = require('crypto');

const cryptoHash =(...inputs) => {
    const hash = crypto.createHash('sha256');
    hash.update(inputs.sort().join(' '));
    return hash.digest('hex');
}

module.exports = cryptoHash;
```

JS blockchain.js > ...

```
const Block = require('./block');

class Blockchain {

    constructor() {
        this.chain = [Block.genesis()];
    }

    addBlock({ data }) {
        const newBlock = Block.mineBlock({
            lastBlock: this.chain[this.chain.length-1],
            data


        });

        this.chain.push(newBlock);
    }

}

module.exports = Blockchain;

```

```
addSmartContract({data}) {
    console.log("hellooo");
    const parsedata = data.split(',');

    if ((parsedata[0] !== "SC1") && (parsedata[0] !== "SC2") && (parsedata[0] !== "SC3")) {

        console.log("the type");
        return false;

    }

    var letters = /^[A-Za-z ]+$/;

    for(let i=0; i<parsedata[1].length; i++){
        if(parsedata[1][i].match(letters) == false && parsedata[1][i] != ' ' ){
            console.log("ERROR Name: ", parsedata[1]);
        return false;
        }
    }

    if (parsedata[0] !== "SC1") {

        if (parsedata[2].match(/^\d\d[/]\d\d[/]\d\d\d\d $/)) {
            console.log("dob is wrong");
            return false;
        }
        if(parsedata[3].match(/^\d{12}$/)){
            console.log("id is wrong");
            return false;
        }
    }
    else{
        if (parsedata[2].match(/^[A-Za-z]+$/)) {
            console.log("location is wrong");
            return false;
        }
        if(parsedata[3].match(/^\d{5}$/)){
            console.log("id is wrong");
            return false;
        }
    }

    this.addBlock({data});

    console.log("This works!");

}
```

JS server.js > ...

```
const Blockchain = require('./blockchain');
const Block = require('./block');

const blockchain = new Blockchain();

const newData1 = 'Terry Williams, 05/05/1995, 154123681740';
const newData2 = 'Candice Yang, 01/23/1965, 194267895130';
const newData3 = 'Jerry Parker, 03/29/1999, 193579272416';
const newData4 = 'Jack Jackson, 03/29/1999, 161547861784';
const newData5 = 'Tommy Lee, 03/29/1999, 116154896164';

blockchain.addBlock({data: newData1});
blockchain.addBlock({data: newData2});
blockchain.addBlock({data: newData3});
blockchain.addBlock({data: newData4});
blockchain.addBlock({data: newData5});

const newSCdata1 = 'SC1,Tim Juniour,02/23/1990,124569871561';
const newSCdata2 = 'SC2,Jessica Hollins,Halifax,14597';
const newSCdata3 = 'SC3,Harry West,Toronto,16516';
const newSCdata4 = 'SC1,Frank Victor,05/06/1980,145268745126';
const newSCdata5 = 'SC2,Harry West,Toronto,16516';

blockchain.addSmartContract({data: newSCdata1});
blockchain.addSmartContract({data: newSCdata2});
blockchain.addSmartContract({data: newSCdata3});
blockchain.addSmartContract({data: newSCdata4});
blockchain.addSmartContract({data: newSCdata5});


const used = process.memoryUsage();
for (let key in used) {
  console.log(`${key} ${Math.round(used[key] / 1024 / 1024 * 100) / 100} MB`);
}

var os = require('os');
var cpus = os.cpus();

for(var i = 0, len = cpus.length; i < len; i++) {
    console.log("CPU %s:", i);
    var cpu = cpus[i], total = 0;

    for(var type in cpu.times) {
        total += cpu.times[type];
    }

    for(type in cpu.times) {
        console.log("\t", type, Math.round(100 * cpu.times[type] / total));
    }
}


console.log(blockchain);
```

Appendix B

Application of JavaScript Code (Outputs)

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Abdihakim Mao\Desktop\HealthBlock Code> node server.js


Blockchain {
  chain:
   [ Block {
       timestamp: 1583265132093,
       lastHash: ' ',
       hash:
        '4733596e89a7ebfd4d390e857e3658b67bf1f8f98940f77923028d7f8e233113',
       data: 'John Smith,10/10/1990,19426789510',
       dsign:
        '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
     Block {
       timestamp: 1583265132103,
       lastHash:
        '4733596e89a7ebfd4d390e857e3658b67bf1f8f98940f77923028d7f8e233113',
       hash:
        'a3ce3c84dc8b68bb4abc937e385ef4d1489db92da201c33cc2dc46b52307644b',
       data: 'Terry Williams, 05/05/1995, 154123681740',
       dsign:
        '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
     Block {
       timestamp: 1583265132104,
       lastHash:
        'a3ce3c84dc8b68bb4abc937e385ef4d1489db92da201c33cc2dc46b52307644b',
       hash:
        '2a50c0f70ea28022ad746c44c2a73d20d64111890dc89b1b7c6d9defde06e215',
       data: 'Candice Yang, 01/23/1965, 194267895130',
       dsign:
        '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
     Block {
       timestamp: 1583265132104,
       lastHash:
        '2a50c0f70ea28022ad746c44c2a73d20d64111890dc89b1b7c6d9defde06e215',
       hash:
        '4e5645be7cac2394b0fe9f3659daea6a1bd5edf7fdc312bb3ee305c99f62085b',
       data: 'Jerry Parker, 03/29/1999, 193579272416',
       dsign:
        '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
     Block {
       timestamp: 1583265132104,
       lastHash:
        '4e5645be7cac2394b0fe9f3659daea6a1bd5edf7fdc312bb3ee305c99f62085b',
       hash:
        '9eb5ae9d134f5070c55956a044b2839586aa799efb0821d3c0299f83cfb652c9',
       data: 'Jack Jackson, 03/29/1999, 161547861784',
       dsign:
        '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
     Block {
       timestamp: 1583265132104,
       lastHash:
        '9eb5ae9d134f5070c55956a044b2839586aa799efb0821d3c0299f83cfb652c9',
       hash:
        '5c3bf39eeeafbc44fb706a9f1fe4bbf35787a124f971eddd57ffc4d5f3fc9d23',
       data: 'Tommy Lee, 03/29/1999, 116154896164',
       dsign:
        '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
```

```
Block {
  timestamp: 1583265132109,
  lastHash:
   '5c3bf39eeeafbc44fb706a9f1fe4bbf35787a124f971eddd57ffc4d5f3fc9d23',
  hash:
   'c43e1de7ca32523f5cb2c6f533df267d732e49047ab8186fedb1c89fb3966ed0',
  data: 'SC1,Tim Juniour,02/23/1990,124569871561',
  dsign:
   '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
Block {
  timestamp: 1583265132110,
  lastHash:
   'c43e1de7ca32523f5cb2c6f533df267d732e49047ab8186fedb1c89fb3966ed0',
  hash:
   '18c508da14f5f41389142463ce6777c99db6577de98a3ef46a8945b5dfff4a46',
  data: 'SC2,Jessica Hollins,Halifax,14597',
  dsign:
   '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
Block {
  timestamp: 1583265132111,
  lastHash:
   '18c508da14f5f41389142463ce6777c99db6577de98a3ef46a8945b5dfff4a46',
  hash:
   'faddc1443d91670f77c2915ca0dc35e92e10079f3d0577ce63b4b044adcf74cb',
  data: 'SC3,Harry West,Toronto,16516',
  dsign:
   '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
Block {
  timestamp: 1583265132111,
  lastHash:
   'faddc1443d91670f77c2915ca0dc35e92e10079f3d0577ce63b4b044adcf74cb',
  hash:
   '06229fa60fd31c6f4d16b1c4a735d7a34ef4244117581925a391c302e0541ba7',
  data: 'SC1,Frank Victor,05/06/1980,145268745126',
  dsign:
   '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' },
Block {
  timestamp: 1583265132112,
  lastHash:
   '06229fa60fd31c6f4d16b1c4a735d7a34ef4244117581925a391c302e0541ba7',
  hash:
   '2fa06bb2d577f7aae395069bcc308410cc8d00524bf0410b7620f591e69b65fd',
  data: 'SC2,Harry West,Toronto,16516',
  dsign:
   '8dc4b5c58abe0091d4ddfbbff8803228970b0d1cdc7def679d4c397affe0a5ff' } ] }
```

JS sshare.js > ...

```
var secrets = require("secrets.js-grempe/secrets.js")

var publickey = "MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAecQSkSyGKIr/hMwnCnZSICJty1c/"

var publickeyhex = secrets.str2hex(publickey)
console.log(publickey)

var shares = secrets.share(publickeyhex, 4, 2)
console.log("show all shares:")
console.log(shares[1])
console.log(shares[2])
console.log(shares[3])

var combine = secrets.combine(shares.slice(1,2))

console.log("combine 2 shares:")
console.log(shares[1])
console.log(shares[2])
combine = secrets.combine([shares[1], shares[2]])


combine = secrets.hex2str(combine)
console.log(combine)
console.log(combine === publickey) // => true
```

```
PS C:\Users\Abdihakim Mao\Desktop\HealthBlock Code> node sshare.js
MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAecQSkSyGKIr/hMwnCnZSICJty1c/
show all shares:
801ed8ab4af46d033020d3fac0ad502a1230741a762628c729cdd354c40b4f21ed2fc930df5d0b5426dba6a391abf86088c3fd9fcd0465a4860d80ce
48de512c05a67aa1c5651a15ad1278728260c4b82fa838ec45a546788154994bfd154c4eb110643e1c017212909918d229a34239078706b46f42efd2
1b860d72258cc0ca576
802c70975438cbd66071a0f45b1b7575fcd0e1e531ac4c0e4fea79f986e754b3c7ce5891a6ebda0846269a572a263ca10d87e66e5368c41907dadedd
5f4d7819d1bce8a3872a2c6b4494e8a508f183f191c1bcd9577a83d0dec92f36370a866cbe10c54df382ed852aa3fdc44c768f73d2de0088c1e5c144
2a1c02a442585d2573b
8032a83c1ecca6d5504171fe9d86264fe97092bf432a60f962b7af9d474c1d722ed197417ec6d58c667d3e04bcadc05181f41f8199fca48d87675b23
12832f05d24a961246ef310eeca697a78e814139bb59807516cfc0b85bbdb25dce4fcf320b10a593e9b398f7bcbae1866075cbbad1e9029cab372b86
35da08a660e4998f200
8049312ea860567cc0d346f8ada73fdbe0c1ca0a6ea9558d53a53d62d32ea24783dd7bd3445678a157cd226e4cfc6522070fc05d7e705773d474732b
706b3ba279981ca703a590875649c90a0c030d732cd364b372d4d891a03393dc62f4d3f8b1c187aa3d55c37a4f17e7e887dd0427a87ddce05d7b8db8
4939dcd88df1773aea1
combine 2 shares:
802c70975438cbd66071a0f45b1b7575fcd0e1e531ac4c0e4fea79f986e754b3c7ce5891a6ebda0846269a572a263ca10d87e66e5368c41907dadedd
5f4d7819d1bce8a3872a2c6b4494e8a508f183f191c1bcd9577a83d0dec92f36370a866cbe10c54df382ed852aa3fdc44c768f73d2de0088c1e5c144
2a1c02a442585d2573b
8032a83c1ecca6d5504171fe9d86264fe97092bf432a60f962b7af9d474c1d722ed197417ec6d58c667d3e04bcadc05181f41f8199fca48d87675b23
12832f05d24a961246ef310eeca697a78e814139bb59807516cfc0b85bbdb25dce4fcf320b10a593e9b398f7bcbae1866075cbbad1e9029cab372b86
35da08a660e4998f200
MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAecQSkSyGKIr/hMwnCnZSICJty1c/
true
```

Bibliography

[1] Semigran, H., Levine, D., Nundy, S., & Mehrotra, A. (2016). Comparison of Physician and Computer Diagnostic Accuracy. JAMA Internal Medicine, 176(12), 1860. doi: 10.1001/jamainternmed.2016.6001

[2] Canada, H. (2019). eHealth - Canada.ca. Retrieved 28 November 2019, from https://www.canada.ca/en/health-canada/services/health-care-system/ehealth.html

[3] WHO EHealth Resolution. (2012). Who.int. Retrieved 28 November 2019, from https://www.who.int/ehealth/en/

[4] MLA : For Health Consumers and Patients : Top Health Websites. (2019). Retrieved 28 November 2019, from https://www.mlanet.org/page/top-health-websites

[5] Taber, J., Leyva, B., & Persoskie, A. (2014). Why do People Avoid Medical Care? A Qualitative Study Using National Data. Journal of General Internal Medicine, 30(3), 290-297. doi: 10.1007/s11606-014-3089-1

[6] Admin, E. (2019). EMR, EHR, and PHR – Why All the Confusion? | Canada Health Infoway. Retrieved 28 November 2019, from https://www.infoway-inforoute.ca/en/what-we-do/blog/digital-health-records/6852-emr-ehr-and-phr-why-all-the-confusion

[7] ehr - emr - what are electronic health records?. (2019). Retrieved 28 November 2019, from https://innovatemedtec.com/digital-health/ehr--emr

[8] Blockchain 101 - CoinDesk. (2019). Retrieved 28 November 2019, from https://www.coindesk.com/learn/blockchain-101/what-is-blockchain-technology

[9] (2019). Retrieved 28 November 2019, from https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu_impact-blockchain-fund-distribution.pdf

[10] (2019). Retrieved 28 November 2019, from https://study.com/academy/lesson/what-is-cryptography-definition-uses.html

[11] What Is Public-Key Cryptography?. (2019). Retrieved 28 November 2019, from https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/

[12] Peer-to-Peer Networks Explained | Binance Academy. (2019). Retrieved 28 November 2019, from https://www.binance.vision/blockchain/peer-to-peer-networks-explained

[13] Blockchain 101 - CoinDesk. (2019). Retrieved 28 November 2019, from https://www.coindesk.com/learn/blockchain-101/what-can-a-blockchain-do

[14] Who Scales It Best? Blockchains' TPS Analysis. (2019). Retrieved 28 November 2019, from https://hackernoon.com/who-scales-it-best-blockchains-tps-analysis-pv39g25mg

[15] Team, D. (2018). Types of Blockchains - Decide which one is better for your Investment Needs - DataFlair. Retrieved 28 November 2019, from https://data-flair.training/blogs/types-of-blockchain/

[16] What Are Smart Contracts? | Binance Academy. (2019). Retrieved 28 November 2019, from https://www.binance.vision/blockchain/what-are-smart-contracts

[17] PDF.js viewer. (2019). Retrieved 28 November 2019, from https://surveys.cma.ca/en/viewer?file=%2fdocuments%2fSurveyPDF%2fCMA_Surv

ey_Workforce2017_Q23_ElectronicToolsUsed-e.pdf#search=%22Q22.%20Use%20of%20electronic%20records%22%20OR%20%22Q23.%20Electronic%20tools%20used%20by%20physicians%22%20OR%20%22Q24.%20Electronic%20tools%20used%20by%20patients%22&phrase=false

[18] PDF.js viewer. (2019). Retrieved 28 November 2019, from https://surveys.cma.ca/en/viewer?file=%2fdocuments%2fSurveyPDF%2fCMA_Survey_Workforce2017_Q22_ElectronicRecords-e.pdf#search=%22Q22.%20Use%20of%20electronic%20records%22%20OR%20%22Q23.%20Electronic%20tools%20used%20by%20physicians%22%20OR%20%22Q24.%20Electronic%20tools%20used%20by%20patients%22&phrase=false

[19] (2019). Retrieved 28 November 2019, from https://www.infoway-inforoute.ca/en/component/edocman/3091-epic-ehr-program-mychart-consumer-health-solutions-benefits-evaluation-report-pilot/view-document?Itemid=101

[20] Ottawa hospitals upgrade medical record system | CBC News. (2019). Retrieved 28 November 2019, from https://www.cbc.ca/news/canada/ottawa/hospitals-ottawa-medical-record-sharing-1.4483264

[21] Health Care Blockchain and Innovative Uses - Freed Associates. (2019). Retrieved 28 November 2019, from https://www.freedassociates.com/insights/point-of-view/innovative-blockchain-uses-in-health-care/

[22] (2019). Retrieved 28 November 2019, from https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

[23] Mayo Clinic exploring blockchain - Ledger Insights. (2018). Retrieved 28 November 2019, from https://www.ledgerinsights.com/mayo-clinic-exploring-blockchain/

[24] Yakubowski, M. (2018). Europe Takes Serious Steps Toward Blockchain Adoption. Retrieved 28 November 2019, from https://cointelegraph.com/news/europe-takes-serious-steps-towards-blockchain-adoption

[25] Abeyratne, S. A., & Monfared, R. P. (2016). Blockchain ready manufacturing supply chain using distributed ledger.

[26] Li, Z., Wang, W. M., Liu, G., Liu, L., He, J., & Huang, G. Q. (2018). Toward open manufacturing: A cross-enterprises knowledge and services exchange framework based on blockchain and edge computing. Industrial Management & Data Systems, 118(1), 303-320.

[27] Kshetri, N. (2018). 1 Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

[28] Wüst, K., & Gervais, A. (2018, June). Do you need a Blockchain?. In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT) (pp. 45-54). IEEE.

[29] Tian, F. (2016, June). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In 2016 13th international conference on service systems and service management (ICSSSM) (pp. 1-6). IEEE.

[30] Korpela, K., Hallikas, J., & Dahlberg, T. (2017, January). Digital supply chain transformation toward blockchain integration. In proceedings of the 50th Hawaii international conference on system sciences.

[31] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

[32] Li, J., Greenwood, D., & Kassem, M. (2018). Blockchain in the built environment: analysing current applications and developing an emergent framework. Diamond Congress Ltd.

[33] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 36, 55-81.

[34] Castaldo, L., & Cinque, V. (2018, February). Blockchain-based logging for the cross-border exchange of ehealth data in europe. In International ISCIS Security Workshop (pp. 46-56). Springer, Cham.

[35] Genestier, P., Zouarhi, S., Limeux, P., Excoffier, D., Prola, A., Sandon, S., & Temerson, J. M. (2017). Blockchain for consent management in the ehealth environment: A nugget for privacy and security challenges. Journal of the International Society for Telemedicine and eHealth, 5, GKR-e24.

[36] Kuo, T. T., Kim, H. E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6), 1211-1220.

[37] Ahmed, T., Bloom, G., Iqbal, M., Lucas, H., Rasheed, S., Waldman, L., ... & Bhuiya, A. (2014). E-health and M-Health in Bangladesh: Opportunities and Challenges (No. IDS Evidence Report; 60). IDS.

[38] Mettler, M. (2016, September). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-3). IEEE.

[39] Weiss, M., Botha, A., Herselman, M., & Loots, G. (2017, May). Blockchain as an enabler for public mHealth solutions in South Africa. In 2017 IST-Africa Week Conference (IST-Africa) (pp. 1-8). IEEE.

[40] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017, September). How blockchain could empower ehealth: An application for radiation oncology. In VLDB Workshop on Data Management and Analytics for Medicine and Healthcare (pp. 3-6). Springer, Cham.

[41] Shen, B., Guo, J., & Yang, Y. (2019). MedChain: Efficient Healthcare Data Sharing via Blockchain. Applied Sciences, 9(6), 1207.

[42] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.

[43] Samavi, R., Doyle, T. E., & Topologlou, T. (2017, November). The first workshop on blockchain & eHealth: towards provable privacy & security in data intensive health research. In Proceedings of the 27th Annual International Conference on Computer Science and Software Engineering (pp. 333-336). IBM Corp.

[44] Rifi, N., Rachkidi, E., Agoulmine, N., & Taher, N. C. (2017, October). Towards using blockchain technology for eHealth data access management. In 2017 Fourth

International Conference on Advances in Biomedical Engineering (ICABME) (pp. 1-4). IEEE.

[45] Zhang, X., & Poslad, S. (2018, May). Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In 2018 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[46] Theodouli, A., Arakliotis, S., Moschou, K., Votis, K., & Tzovaras, D. (2018, August). On the design of a Blockchain-based system to facilitate Healthcare Data Sharing. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1374-1379). IEEE.

[47] Alexaki, S., Alexandris, G., Katos, V., & Petroulakis, E. N. (2018, September). Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions. In 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD) (pp. 1-6). IEEE.

[48] Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018, June). Blochie: a blockchain-based platform for healthcare information exchange. In 2018 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 49-56). IEEE.

[49] Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., & Ylianttila, M. (2018, September). Blockchain Utilization in Healthcare: Key Requirements and Challenges. In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-7). IEEE.

[50] Zhang, P., Walker, M. A., White, J., Schmidt, D. C., & Lenz, G. (2017, October). Metrics for assessing blockchain-based healthcare decentralized apps. In 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-4). IEEE.

[51] Zheng, X., Mukkamala, R. R., Vatrapu, R., & Ordieres-Mere, J. (2018, September). Blockchain-based personal health data sharing system using cloud storage. In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-6). IEEE.

[52] Sun, Y., Zhang, R., Wang, X., Gao, K., & Liu, L. (2018, July). A decentralizing attribute-based signature for healthcare blockchain. In 2018 27th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-9). IEEE.

[53] Randall, D., Goel, P., & Abujamra, R. (2017). Blockchain applications and use cases in health information technology. J Health Med Informat, 8(276), 2.

[54] Hussen, H. M. (2018). A Blockchain-based Service Provider Validation and Verification Framework for Healthcare Virtual Organization. UHD Journal of Science and Technology, 2(2), 24-31.

[55] Gheorghiu, B., & Hagens, S. (2016). Measuring interoperable EHR adoption and maturity: a Canadian example. BMC medical informatics and decision making, 16(1), 8.

[56] Tharmalingam, S., Hagens, S., & Zelmer, J. (2016). The value of connected health information: perceptions of electronic health record users in Canada. BMC medical informatics and decision making, 16(1), 93.

[57] Koeppl, T. V., & Kronick, J. (2017). Blockchain Technology–What's in Store for Canada's Economy and Financial Markets?. CD Howe Institute Commentary, 468.

[58] Wolfond, G. (2017). A blockchain ecosystem for digital identity: improving service delivery in Canada’s public and private sectors. Technology Innovation Management Review, 7(10).

[59] Carrnadin, A. (2018). Achieving Meaningful Use of Electronic Health Records: Prospects for Blockchain in Ontario's Health Care System.

[60] Ducas, E., & Wilner, A. (2017). The security and financial implications of blockchain technologies: Regulating emerging technologies in Canada. International Journal, 72(4), 538-562.

[61] Munster, J., & Jacobsen, H. A. (2018, June). Secret sharing in pub/sub using trusted execution environments. In Proceedings of the 12th ACM International Conference on Distributed and Event-based Systems (pp. 28-39). ACM.

[62] Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 41(10), 1027-1038.

[63] Novikov, S. P., Kazakov, O. D., Kulagina, N. A., & Azarenko, N. Y. (2018, September). Blockchain and Smart Contracts in a Decentralized Health Infrastructure. In 2018 IEEE International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS) (pp. 697-703). IEEE.

[64] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of medical systems, 42(7), 130.

[65] Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2017). Applying software patterns to address interoperability in blockchain-based healthcare apps. arXiv preprint arXiv:1706.03700.

[66] Choudhury, O., Sarker, H., Rudolph, N., Foreman, M., Fay, N., Dhuliawala, M., ... & Das, A. K. (2018). Enforcing human subject regulations using blockchain and smart contracts. Blockchain in Healthcare Today.

[67] Tang, H., Tong, N., & Ouyang, J. (2018, August). Medical Images Sharing System Based on Blockchain and Smart Contract of Credit Scores. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN) (pp. 240-241). IEEE.

[68] Hu, Y., Liyanage, M., Mansoor, A., Thilakarathna, K., Jourjon, G., Seneviratne, A., & Ylianttila, M. (2018). The Use of Smart Contracts and Challenges. arXiv preprint arXiv:1810.04699.

[69] Li, B. (2017). Blockchain and smart contracts in health-related MyData scenario.

[70] Bergquist, J. (2017). Blockchain Technology and Smart Contracts: Privacy-Preserving Tools.

[71] Raman, R. K., & Varshney, L. R. (2018, February). Distributed storage meets secret sharing on the blockchain. In 2018 Information Theory and Applications Workshop (ITA) (pp. 1-6). IEEE.

[72] Anwar, H., & Anwar, H. (2018). The Ultimate Comparison of Different Types of Distributed Ledgers: Blockchain vs Hashgraph vs Dag vs Holochain. Retrieved 28 November 2019, from https://101blockchains.com/blockchain-vs-hashgraph-vs-dag-vs-holochain/

[73] Blockchain Public / Private Key Cryptography in a nutshell. (2018). Retrieved 28 November 2019, from https://medium.com/coinmonks/blockchain-public-private-key-cryptography-in-a-nutshell-b7776e475e7c

[74] How To Create Blockchain In JavaScript. (2018). Retrieved 1 October 2019, from https://appdividend.com/2018/12/15/how-to-create-blockchain-in-javascript/

[75] secrets.js-grempe. (2019). Retrieved 1 October 2019, from https://www.npmjs.com/package/secrets.js-grempe#examples

[76] SHA-256 hash calculator | Xorbin. (2019). Retrieved 1 November 2019, from https://xorbin.com/tools/sha256-hash-calculator

[77] Chum, C. S., & Zhang, X. (2015). Implementations of a Hash Function Based Secret Sharing Scheme. Journal of Applied Security Research, 10(4), 525-542.

[78] Alapati, K. K. (2018). Group-oriented secret sharing using Shamir's algorithm (Doctoral dissertation, Rutgers University-Camden Graduate School).

[79] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613.

[80] Blakley, G. R. (1979, June). Safeguarding cryptographic keys. In 1979 International Workshop on Managing Requirements Knowledge (MARK) (pp. 313-318). IEEE.