6-2023

BLOCKCHAIN-ENABLED EHR SHARING IN HEALTHCARE FEDERATION: SHARDING AND INTERBLOCKCHAIN COMMUNICATION

Faiza Hashim
United Arab Emirates University, 201890063@uaeu.ac.ae

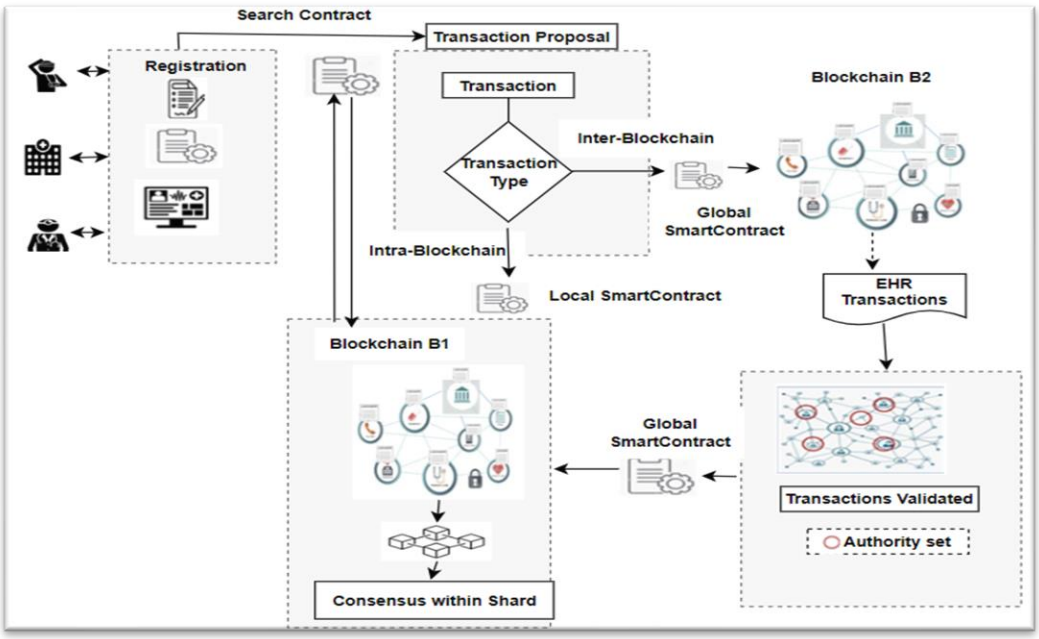
جامعة الإمارات العربية المتحدة
United Arab Emirates University

DOCTORATE DISSERTATION NO. 2023: 35

College of Information Technology

BLOCKCHAIN-ENABLED EHR SHARING IN HEALTHCARE FEDERATION: SHARDING AND INTER-BLOCKCHAIN COMMUNICATION

Faiza Hashim



June 2023

United Arab Emirates University

College of Information Technology

BLOCKCHAIN-ENABLED EHR SHARING IN HEALTHCARE FEDERATION: SHARDING AND INTER-BLOCKCHAIN COMMUNICATION

Faiza Hashim

This dissertation is submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Informatics and Computing

June 2023

United Arab Emirates University Doctorate Dissertation

2023: 35

Cover: Image regarding healthcare blockchain federation in this study

(Photo: By Faiza Hashim)

Print: University Print Service, UAEU 2023

Declaration of Original Work

I, Faiza Hashim, the undersigned, a graduate student at the United Arab Emirates University (UAEU), and the author of this dissertation entitled "*Blockchain-Enabled EHR Sharing in Healthcare Federation: Sharding and Inter-Blockchain Communication*", hereby, solemnly declare this is the original research work done by me under the supervision of Prof. Khaled Shuaib, at the College of Information Technology at UAEU. This work has not previously formed the basis for the award of any academic degree, diploma, or similar title at this or any other university. Any materials borrowed from other sources (whether published or unpublished) and relied upon or included in my dissertation have been properly cited and acknowledged in accordance with appropriate academic conventions. I further declare that there is no potential conflict of interest with respect to the research, data collection, authorship, presentation, and/or publication of this dissertation.

Student's Signature: 

Date: June 16, 2023

Advisory Committee

1) Advisor: Dr. Khaled Shuaib

Title: Professor

Department of Information Systems and Security

College of Information Technology

2) Member: Dr. Nazar Zaki

Title: Professor

Department of Computer Science and Software Engineering

College of Information Technology

3) Member: Dr. Farag Sallabi

Title: Associate Professor

Department of Computer and Network Engineering

College of Information Technology

Approval of the Doctorate Dissertation

This Doctorate Dissertation is approved by the following Examining Committee Members:

1) Advisor (Committee Chair): Dr. Khaled Shuaib
   Title: Professor
   Department of Information Systems and Security
   College of Information Technology

   Signature  Date: June 16, 2023

2) Member: Dr. Mohammad Mehedy Masud
   Title: Associate Professor
   Department of Information Systems and Security
   College of Information Technology

   Signature  Date: June 16, 2023

3) Member: Dr. Fady Alnajjar
   Title: Associate Professor
   Department of Computer Science and Software Engineering
   College of Information Technology

   Signature  Date: June 16, 2023

4) Member: Dr. Nidal Nasser
   Title: Professor
   Department of Software Engineering
   College of Engineering,
   Alfaisal University, Riyadh, KSA

   Signature  Date: June 16, 2023

This Doctorate Dissertation is accepted by:

OBO/
Dean of the College of Information Technology: Professor Taieb Znati

Signature _____

Date: 23/08/2023

Dean of the College of Graduate Studies: Professor Ali Al-Marzouqi

Signature Ali Hassan

Date: 23/08/2023

Abstract

Electronic Health Records (EHRs) are crucial components of the healthcare system, facilitating accurate and efficient diagnosis. Blockchain technology has emerged as a promising solution to improve EHRs sharing among medical practitioners while ensuring privacy and security. By leveraging its decentralized, distributed, immutable, and secure architecture, blockchain has the potential to revolutionize the healthcare system. However, due to security concerns, blockchain networks in healthcare typically operate in private or consortium modes, resulting in isolated networks within a federation. Scalability remains a significant challenge for blockchain networks, as the number of participating nodes increases within each network of the federation. Consensus mechanisms in blockchain networks establish rules for maintaining a unified view of the ledger, enabling all nodes access to the same information. Additionally, achieving interoperability between independent blockchain networks, whether homogeneous or heterogeneous, poses a major obstacle for healthcare providers seeking to share EHRs across a large-scale blockchain federation. This research aims to address these challenges by developing a blockchain federation model for EHRs sharing in healthcare. The primary contributions include resolving scalability issues in healthcare blockchain networks through a transaction-based sharding technique and proposing an enhanced Proof-of-Authority (PoA) consensus algorithm for scalable authority selection. Furthermore, this research aims to tackle interoperability challenges among independent blockchains by introducing transaction-based inter-blockchain communication and leveraging global and local smart contracts. Experimental results demonstrate the significance of the proposed methods in addressing scalability and interoperability challenges within a blockchain federation, enabling efficient patient EHR sharing within the network and across independent blockchain networks deployed on various platforms.

Keywords: Healthcare blockchain, electronic health record sharing, consensus, scalability, interoperability, sharding, healthcare blockchain federation, inter-blockchain communication.

Title and Abstract (in Arabic)

مشاركة السجلات الصحية الإلكترونية بواسطة الكتل المتسلسلة باستخدام التجزئة والاتصال بين الكتل المتسلسله في اتحاد الرعاية الصحية

الملخص

تعد السجلات الصحية الإلكترونية (EHR) أصولًا مهمة لنظام الرعاية الصحية وتحتاج إلى مشاركتها بين الممارسين الطبيين لتحسين دقة وكفاءة التشخيص. تم التحقيق في تقنية الكتل المتسلسلة واعتمادها في مجال الرعاية الصحية كحل لمشاركة السجلات الصحية الإلكترونية التي تتيح الحفاظ على الخصوصية والأمن. يمكن للكتل المتسلسلة إحداث ثورة في نظام الرعاية الصحية من خلال توفير بنية لامركزية وموزعة وغير قابلة للتغيير وآمنة. نظرًا لمخاوف الأمان والخصوصية للرعاية الصحية، يتم اعتماد شبكات blockchain في أوضاع خاصة / اتحاد؛ وبالتالي، تعمل العديد من شبكات الكتل المتسلسلة في صوامع لتشكيل اتحاد. لطالما كانت قابلية التوسع تمثل عنق الزجاجة في شبكات الكتل المتسلسلة، حيث يميل عدد العقد المشاركة إلى الزيادة في كل شبكة داخل الاتحاد. تحدد آلية الإجماع في الكتل المتسلسلة قواعد العقد المتصلة للاتفاق على الحفاظ على عرض واحد للموازنة مع معاملات صالحة بين جميع الأقران بحيث يمكن للجميع الوصول إلى نفس المعلومات. علاوة على ذلك، يشكل تحقيق إمكانية التشغيل البيني بين شبكات الكتل المتسلسلة المستقلة (المتجانسة وغير المتجانسة) عقبة كبيرة أمام مقدمي الرعاية الصحية الذين يسعون إلى مشاركة السجلات الصحية الإلكترونية عبر اتحاد الكتل المتسلسلة واسعة النطاق. يهدف هذا البحث إلى تطوير اتحاد الكتل المتسلسلة لنموذج مشاركة السجلات الصحية الإلكترونية في الرعاية الصحية. أولاً ،تتمثل المساهمة الرئيسية لهذا البحث في معالجة مسألة قابلية التوسع في شبكات الكتل المتسلسلةللرعاية الصحية باستخدام تقنية التجزئة القائمة على المعاملات. ثانيًا، نقترح خوارزمية إجماع محسّنة لإثبات السلطة (PoA) لمشاركة السجلات الصحية الإلكترونية لتوفير آلية قابلة للتطوير لاختيار السلطة في خوارزميات إجماع PoA. أخيرًا، يهدف هذا البحث إلى حل تحديات التشغيل البيني بين الكتل المتسلسلة المستقلة باستخدام الاتصالات بين الكتل المتسلسلة القائمة على المعاملات لمشاركة EHR في اتحاد من الكتل المتسلسلة من خلال دمج مفهوم العقود الذكية العالمية والمحلية في الشبكة. تُظهر النتائج التجريبية أهمية أساليبنا المقترحة في معالجة تحديات قابلية التوسع وقابلية التشغيل البيني في اتحاد الكتل المتسلسلة لمشاركة EHR للمريض داخل الشبكة وعبر شبكات الكتل المتسلسلة المستقلة المنتشرة عبر منصات الكتل المتسلسلة المختلفة.

الكلمات الرئيسية: الكتل المتسلسلة للرعاية الصحية، مشاركة السجلات الصحية الإلكترونية، الإجماع، قابلية التوسع، إمكانية التشغيل البيني، التجزئة، اتحاد الكتل المتسلسلة للرعاية الصحية، الاتصال بين الكتل المتسلسلة.

List of Publications

This dissertation is based on the work presented in the following papers, referred to by Roman numerals.

I. Hashim, F., Shuaib, K., and Sallabi, F., "MedShard: Electronic Health Record Sharing Using Blockchain Sharding," *Sustain. 2021,* pp. 5889, vol. 13, no. 11, May 2021, doi: 10.3390/SU13115889.

II. Hashim, F., Shuaib, K. and Sallabi, F., "Performance Evaluation of Blockchain Consensus Algorithms for Electronic Health Record Sharing. In *2021 Global Congress on Electrical Engineering (GC-ElecEng)*, IEEE, pp. 136-143, December 2021.

III. Hashim, F., Shuaib, K., and Sallabi, F., "Connected Blockchain Federations for Sharing Electronic Health Records," *Cryptogr. 2022,* pp. 47, vol. 6, no. 3, Sep. 2022, doi: 10.3390/CRYPTOGRAPHY6030047.

IV. Hashim, F., Shuaib, K., Baraka, E., and Sallabi, F., **"**Integration of heterogeneous blockchains for sharing EHRs using transaction-based global smart contracts"**.** (Submitted manuscript)

Author's Contribution

The contribution of Faiza Hashim to the papers included in this dissertation was as follows:

I. Identified and outlined the dissertation goals and developed the healthcare blockchain federation for sharing EHRs between independent networks and sharding solutions in individual blockchain networks.

II. Participated in planning of the work and had the main responsibility for the development of proposed networks, experimental work, evaluation of results, and manuscript writing.

III. Sole responsibility for planning the research, conducting the experiments, and preparing the dissertation.

Author Profile

Faiza Hashim is a highly motivated PhD candidate at UAE University in Al Ain, UAE. She holds a bachelor’s degree in computer science, a master's, and an MPhil degree in Information Technology from the University of Peshawar, Pakistan.

With a keen interest in cutting-edge technologies, Faiza's research revolves around the fields of smart healthcare, blockchain networks, artificial intelligence, machine learning, and natural language processing. Currently, she serves as a senior research assistant, actively contributing to a healthcare blockchain project. In pursuit of her PhD, Faiza's primary focus lies in the healthcare blockchains federation for the seamless sharing of EHRs. During her PhD studies, Faiza has made notable contributions to her field, publishing high-quality articles as the first author in top-tier journals and conferences, thereby showcasing her expertise and research capabilities. Her work demonstrates a strong commitment to advancing knowledge in her area of specialization.

Faiza is also an accomplished teaching assistant at UAE University, having successfully completed the PhD teaching academy course. Her teaching role allows her to share her expertise with students, helping them grasp complex concepts and develop their skills in computer science and related disciplines.

Acknowledgments

First and foremost, I would like to express my deepest gratitude to Allah for granting me the faith, strength, and abilities needed to complete my PhD journey.

I would like to extend my heartfelt appreciation to my advisor, Prof. Khaled Shuaib, for his exceptional guidance, unwavering support, valuable insights, and encouragement throughout my entire PhD research and the preparation of this dissertation. Working under his supervision has been an honor, and I eagerly anticipate the opportunity to continue collaborating with him in the future.

I am also immensely grateful to my esteemed advisory committee members, Prof. Nazar Zaki and Dr. Farag Sallabi, for their invaluable guidance, expert advice, and their willingness to address any challenges I encountered during my research. I would also like to extend my sincere appreciation to Prof. Mohammed Adil Serhani for his support, guidance, and motivation during my PhD journey. I am grateful to all the faculty at the College of Information Technology for their support and valuable input. My heartfelt thanks go out to my friends and colleagues at the United Arab Emirates University, whose companionship and support have made this journey memorable and meaningful.

I owe an immeasurable debt of gratitude to my parents for their constant prayers and unwavering belief in me. I am also deeply grateful to my siblings for their unconditional support and encouragement throughout this endeavor. Additionally, I am profoundly grateful to my children, Muhammad Ali Yar, Azlan Hashim, and Inaaya Hashim, for their understanding, patience, and the space they provided me to complete my research.

Last but certainly not least, I want to express my deepest appreciation to my beloved husband, Muhammad Hashim Yar, for his immeasurable love, unwavering support, and unshakeable belief in me. Without his constant encouragement and assistance, this achievement would not have been possible.

Once again, I extend my sincere gratitude to all those who have played a part in shaping my academic journey, and I am truly blessed to have had such incredible support throughout my PhD studies.

Dedication

To my beloved parents, loving husband, and my adorable kids

Table of Contents

List of Tables

List of Figures

List of Abbreviations

B_N	Blockchain Nodes
CA	Certificate Authority
CG	Caregiver
CT	Communication Time
EHR	Electronic Health Record
ET	Elapsed Time
HLF	Hyperledger Fabric
IoT	Internet of Things
IPFS	Inter Planetary File System
LT	Latency
MoH	Ministry of Health
PBFT	Practical Byzantine Fault Tolerance
PoA	Proof of Authority
PoS	Proof of Stake
PoW	Proof of Work
QT	Query Processing Time
S_N	Shard Nodes
TP	Throughput

Chapter 1: Introduction

1.1 Overview

Blockchain is a dominant technology that enables secure, immutable, authorized, authenticated, and trusted data sharing in a distributed network without the involvement of a third party. The researcher/scholar known as Satoshi Nakamoto presented the concept of blockchain as the underlying technology of Bitcoin in a white paper published in 2009 [1]. Blockchain is a distributed database and maintains a continuously growing list of records, called blocks. Every block is connected to another block by maintaining the hash of the previous block in the chain. This chain of blocks provides a tamper-proof database such that once a block is added to the chain, it cannot be edited or changed.

Based on the scope of participants in a blockchain network, three categories are identified [2, 3, 4], namely, public, private, and consortium blockchains. Public blockchains are also referred to as permissionless blockchains, as anyone is allowed to join and participate in the validation and mining process of block generation. Private blockchains are permissioned blockchains, sole-owned by an organization or entity which strictly controls and monitors participants. Consortium blockchains are formed by a consortium of multiple organizations or entities to create a peer-to-peer network. A consortium blockchain can be considered a blockchain of multiple private blockchains [4]. In private and consortium blockchains, miners are predefined, and participation in the network is controlled. In a consortium blockchain, multiple members share the ownership and control authority.

The efficacious implementation of Bitcoin has appealed to various domains, and the appeal of this distributed and trusted technology has spread beyond the Bitcoin network. Currently, blockchain technology is extensively and effectively used in diverse applications and industries, such as prediction markets [5, 6], financial engineering [7, 8], automated reasoning systems [9], smart contract-based systems [10], healthcare [3, 11], energy [12, 13], supply chains [14, 15], and agriculture [16, 17].

The focus of the current study is the healthcare blockchain used to share the EHR of patients in the network. Blockchain technology is projected to transform the healthcare ecosystem through its distinct characteristics, which include decentralization, security, immutability, persistency, anonymity, and auditability. Blockchain can reshape traditional

EHR sharing across multiple healthcare entities, thus improving the quality of healthcare by making it smarter and more efficient. Patients with multiple Caregivers (CGs) need to share their medical history effectively for better service. Thus, it is important to share health records among various stakeholders of the healthcare ecosystem, including individuals (patients and their CGs) and individuals and a stakeholder (patients and insurance companies/research centers). Sharing EHR is an important step in expanding the interoperability of healthcare providers and making the healthcare system smart and efficient.

EHR-sharing systems are increasingly being used to share patient data among various healthcare stakeholders (including hospitals, CGs, laboratories, pharmacies, insurance companies, researchers, and patients). Traditional centralized systems have been used for healthcare EHR interoperability, but the centralized model has some drawbacks as the network grows. Recently, blockchain-based EHR sharing has been used extensively in the literature to overcome the limitations of centralized healthcare systems. The high-level comparison presented below highlights the limitations of the centralized model and the solutions that the blockchain model offers in healthcare:

- Single point of failure: In a centralized healthcare model, patient data is stored in a centralized database. Any failure of the database results in the loss of all EHRs. In a second scenario, EHRs are stored on the premises of individual facilities and shared through a centralized entity. A failure of the central entity results in a failure of the communication channel. In contrast, in a blockchain-based model EHRs are replicated in a common ledger for all healthcare facilities and do not have a single point of failure problem.
- Centralized power: In a centralized model, hospital A must send a request to hospital B through a centralized authority. This leads to delays in executing requests as the network grows. However, blockchain provides a peer-to-peer network where hospital A can send a request to hospital B for patient data.
- Single decision-making authority: In a centralized model, a single authority manages the network. The rules for decision making and the flow of data requests in the network are handled solely by the centralized entity, with no concern for the network nodes. To address this limitation, blockchain provides a decentralized network where

network rules are set based on majority consensus and decision making is extended to all network nodes.

- Interoperability: In a centralized model, the patient record is maintained by each hospital in a heterogeneous data format, leading to interoperability issues. A blockchain-distributed ledger solves this problem by replicating the single view of the ledger to all network nodes.
- Security: Security is a major concern in centralized systems as they are exposed to various cyberattacks that can lead to data breaches. Blockchain provides immutability and integrity for health data through encryption and hashing techniques in the distributed ledger.

Blockchain technology implements distributed ledgers in healthcare and provides decentralization and interoperability. However, blockchain networks are mostly deployed using private or consortium models due to the security and privacy issues surrounding healthcare records, which cannot be exposed in a public network. Various healthcare blockchains thus function in silos, creating fragmentation in healthcare systems as well as interoperability challenges as independent blockchain networks share the EHRs of patients visiting multiple clinics but residing in different blockchains due to the geographic locations and rules in force in a state.

The blockchain federation consists of multiple independent networks deployed via different blockchain platforms, each of which has a distinct business logic, rules, healthcare entities, transaction format, and validation process. This study focuses on sharing patient EHRs in a federation of blockchains and addresses the scalability and interoperability challenges in implementing blockchains in a healthcare federation. Healthcare is a fast-growing and dynamic network of nodes because nodes may join at a high rate, which can lead to network degradation and transaction delays due to the consensus mechanism used among them. Thus, healthcare blockchain networks should be scalable as the number of nodes increases in the network.

In this study, first, scalability is addressed at the single network level in a federation. The proposed solutions are functional at the appointment level, that is, once the appointment between the patient and CG starts at the clinic. To overcome the scalability challenges in individual blockchains, we propose sharding in healthcare by using a novel technique for

shard formation, “transaction-based sharding,” and processing each appointment within the shard. The two main challenges of sharding are addressed in this study, namely, shard formation and cross-shard communication, which are linked as the shard formation affects the cross-shard communication process. Currently, clustering techniques are used for shard formation that result in nodes in one shard communicating with nodes in another. This delays the transaction processing in the network and reduces network Throughput (TP).

We also improve the PoA consensus algorithm for healthcare by providing a mechanism for authority selection. Our proposed method selects a minimal set of authorities yet provides equal opportunities for all healthcare entities to be candidates for the authority set and solves the scalability issues of blockchains in healthcare.

The interoperability between independent blockchains is at an embryonic stage, and related research is ongoing. In this research study, we propose a solution for inter-blockchain communication in a healthcare blockchain federation to share EHR by using a novel technique, “transaction-based inter-blockchain communication,” which uses a global and local smart contracts technique among homogeneous and heterogeneous healthcare networks.

1.2 Statement of the Problem

The effective sharing of medical history of patients with multiple care providers is crucial for delivering optimal healthcare services. Seamless sharing of EHRs across various stakeholders within the healthcare ecosystem, including patients, care providers, insurance companies, and research centers, is essential for achieving interoperability and improving the efficiency of the healthcare system. However, scalability issues present significant challenges in rapidly growing healthcare blockchain networks, as network performance deteriorates with an increasing number of participants. This degradation in performance leads to delays in transaction verification, which is unacceptable in the sensitive healthcare environment. Therefore, healthcare blockchain networks require efficient, real-time, and scalable consensus algorithms to enhance their performance and minimize consensus time.

Furthermore, achieving interoperability in the healthcare domain is crucial for enabling the sharing of EHRs among patients residing in independent blockchain networks. Each blockchain network may have its own distinct rules and regulations, posing obstacles to the exchange of EHRs when needed for accurate diagnosis and treatment. These challenges are particularly prominent when patients receive healthcare services from providers located in different countries, regions, or even within a single country with diverse sets of regulations per state or emirate. Establishing a federation of properly communicating blockchain networks would effectively address these issues and better serve the needs of all stakeholders involved in healthcare delivery.

1.3 Research Objectives

This dissertation significantly contributes to the advancement of the state of the art by offering innovative solutions to address the scalability challenges in healthcare blockchains and establish efficient methods for securing EHRs sharing within the same blockchain and across blockchain federations. The research makes the following noteworthy contributions:

1.3.1 Objective One

In pursuit of this objective, the research presents the following contributions:

- Scaling up blockchain-based systems in healthcare through sharding.
- Proposing a novel approach called "transaction-based shard formation," where patient identification, represented by a cryptographic public key, determines shard membership based on previous visits to CGs. This eliminates the need for patients to maintain visit records.
- Mitigating the overhead of cross-shard communication by creating complete shards for each appointment, ensuring that nodes within a shard do not require communication with nodes in other shards.

1.3.2 Objective Two

The research contributes to this objective through the following advancements:

- Proposing an improved Proof of Authority (PoA) consensus algorithm tailored for healthcare blockchains. This algorithm utilizes instantaneous authority selection for each appointment.
- Selecting authority nodes dynamically based on the patient's previous records, which helps in selecting a minimum number of authorities in consensus process.
- The proposed authority selection process remains unaffected by network growth.

1.3.3 Objective Three

In pursuit of this objective, the research presents the following contributions:

- Proposing a blockchain network for sharing EHRs among independent and homogeneous blockchain networks within a federation.
- Developing a novel healthcare blockchain integration model that employs transaction-based inter-blockchain communication to facilitate EHRs sharing within a federation of independent blockchains.
- Leveraging local and global smart contracts to establish communication links and facilitate transaction flow within the blockchain federation.

1.3.4 Objective Four

The research makes the following contributions to achieve this objective:

- Extending the scope of EHRs sharing in healthcare blockchain network models to include independent and heterogeneous networks within a federation.
- Introducing a cross-chain communication protocol that integrates heterogeneous blockchains using a transaction-based global smart contract triggering system.
- Proposing a uniform conversion module within the global smart contract to ensure compatibility of transactions across diverse blockchain network platforms.

These contributions significantly advance the field of healthcare blockchains, addressing scalability concerns, enhancing EHRs sharing capabilities, and enabling seamless integration between independent blockchain networks within federations. The proposed solutions have the potential to revolutionize healthcare systems and improve patient care outcomes.

1.4 Relevant Literature

Blockchain technology is projected to transform the healthcare ecosystem with its distinct characteristics, which include decentralization, security, immutability, persistency, anonymity, and audibility. Blockchain can reshape traditional EHRs sharing across multiple healthcare entities to make healthcare smarter and more efficient. Blockchain has revolutionized healthcare and been adopted in projects including MedRec [18], MedicalChain [19], Healthcare Data Gateway (HGD) [20], MedBlock [21], and Medchain [22]. However, scalability poses a major challenge and needs to be addressed to ensure efficient and speedy data sharing in healthcare. Scalability is defined as follows: As the number of transactions grows, the system becomes slower, more expensive, and less sustainable over the long term. Accordingly, previous research addressing blockchain network scalability and interoperability using sharding, consensus algorithms, and inter-blockchain communication protocols is discussed in the following subsections.

1.4.1 Sharding-based Healthcare Blockchain

Sharding is a database technique successfully adopted in blockchain technology to resolve the scalability issue. This technique splits the transaction processing overhead among various small groups of nodes (called committees or shards). These groups work in parallel to improve the network performance with significantly smaller communication, computation, and storage per node, thus permitting the network to scale up to large-size networks [23]. Sharding is a practical solution adopted in several projects from various domains. Elastico [24] was among the first to implement sharding techniques in blockchain, followed by Omniledger [25], Chainspace [26], Rapidchain [23], and Monoxide [27].

Healthcare has welcomed blockchain technology for EHRs management and secure sharing across the participating entities in its ecosystem, including patients, CGs, hospitals, laboratories, insurance companies, and pharmaceuticals, as it ensures the distribution of EHRs and provides patients with data ownership [3]. Scalability is a critical challenge in the healthcare blockchain domain as it affects network TP and Latency (LT). Considering that the healthcare system is sensitive to real-time delay, transactional delay causes a serious threat to human life, especially in emergencies. Sharding plays a vital role

in addressing scalability challenges in healthcare by processing patients' appointments in parallel and minimizing the consensus time as consensus is made within each shard. This has a significant impact on the LT and TP of the healthcare blockchain network.

Researchers have been examining the use of sharding in blockchain-based healthcare systems. A multidomain Internet of Things (IoT) blockchain that focuses on blockchain sharding in the healthcare IoT domain was proposed in which each shard included an entity, such as a hospital, and a number of wearable smart devices for medical data collection and distribution among multiple shards (cross-shard communication) [28]. The key limitation of this system is the consensus mechanism that runs twice, first within the shard and then via the main shard, resulting in greater energy consumption and transaction delay.

To address the scalability challenge in blockchain, a lightweight blockchain was proposed by [4] which divided network participants into demographic clusters. Each cluster maintained a single copy of the ledger for the healthcare domain system. The transactions in each cluster were verified by a single miner (Head Blockchain Manager). Although a single miner saves time and energy consumption in the mining process, if they act maliciously shard takeover attacks may occur, causing loss of shard transaction data. Therefore, the mining process should include some trusted nodes to safeguard the shard. A lightweight blockchain maximizes the TP of transactions and reduces energy computation by parallel processing in healthcare blockchains, but it does not effectively address communication among clusters.

Although sharding has not been thoroughly investigated in the healthcare domain, various other domains using sharding to address scalability issues have shown promising results as well as various challenges. Table 1 summarizes sharding projects and indicates strengths and limitations. Currently, the main challenges of sharding relate to communication (cross-shard communication) and security. Further, no blockchain-specific shard formation techniques exist. This study proposes sharding in the healthcare blockchain to efficiently scale healthcare blockchain-based systems to enhance their scalability as the number of blockchain nodes grows in number. A novel technique, "transaction-based sharding," will be used to address scalability in individual blockchains

within a federation. Our proposed method of shard formation will eliminate the cross-shard communication overhead in the network and improve its performance.

Table 1: Summary of projects reviewed on blockchain sharding [29] (© 2023 Springer Nature, reproduced with the permission of Springer Nature)

Index	**Domain**	**Consensus Protocol**	**Features (+ and -)**
[24]	Bitcoin	PBFT	+ Improves throughput and security. + Uses processor identity for shard formation. - Intra-shard communication performed via the final committee. - Consumes energy and time. - Cannot process multi shard transactions.
[25]	NAs	ByzCoinX	+Uses backup strategies that enable the leader to complete or abort cross-shard transactions that are affected by malicious clients. -Relies on clients to proceed with the cross-shard transactions, placing an extra burden on lightweight clients. - Vulnerable to DoS attacks that prevent clients from participating in processing transactions.
[26]	General	MOD-SMART implementation of PBFT	+ Auditing mechanism for tracing malicious participants. + Built-in privacy design. + Support for generic and user-based smart contacts. - Relies on all shards-managing objects being honest. - High rate of aborts under high contention. -Validating transactions can be costly. - Inherits O(n2) messaging complexity owing to its mode of PBFT implementation.
[23]	General	1/3-resiliemt sharding BFT-based blockchain consensus	+ Offers epoch randomness that allows each node to receive a fresh Identity after each epoch-reducing node corruption and takeover. + Efficient routing mechanism for cross-shard transactions verification assumes no trusted setups. + Offers improved scalability measures. - High initialization and storage sharding overhead, which could be problematic in practice owing to high throughput. - double-spending of resources is possible owing to the delay in message exchange because of a DoS attack.
[30]	Accounts	PoW	+ Linear scaling in throughput, storage, efficiency, and security. + Each node stores coded data off the blockchain, and verification is directly performed on the coded data. -Energy consumption due to PoW -higher complexity of decoding

Table 1: Summary of projects reviewed on blockchain sharding [29] (© 2023 Springer Nature, reproduced with the permission of Springer Nature) (Continued)

Index	Domain	Consensus Protocol	Features (+ and -)
[31]	Account	ParoxPBFT	+ Concurrent processing: uses a flattened consensus protocol to order cross-shard transaction. - All clusters share a single view of the ledger. - Waiting time for a new transaction is an overhead
[28]	IoT	PBFT	+ First multidomain IoT blockchain. + Throughput linearly increases as the number of shards increases. - Consensus runs twice - First partitions the blockchain and then merge subblocks for final consensus. - Time-consuming
[32]	IoT		+ Dynamic reward and penalty mechanism to optimize shard validation model. + Enhance throughput. + Control over malicious nodes in each shard. - Fixed number of nodes used in the experiment. -Network scalability should be tested with an increasing number of nodes.
[33]	Accounts	PoW	+ Even distribution of nodes in each shard, which prevents overloading any shard. + Linear scalable using PoW. - Vulnerable to DoS attacks. - Processing time depends on the node's bandwidth, low bandwidth results in high processing time.
[34]	The Internet of Unmanned Vehicles	PoW	+ Lightweight UVs form shards to share computing and communication resources. + Better performance in case the miner is destroyed by enemy forces. + Resource sharing on the battlefield. - UVs battery power is limited, and shard nodes may not fulfill the mining process if UVs run out of power. - Battlefield is dynamic in nature and in this case shard nodes are difficult to maintain.
[35]	Healthcare	PoA	+ Scalable EHR sharing using sharding. +Real-time nodes assignment to shards based on patient's previous medical history. - Threat models need to be defined for better performance.

Table 1: Summary of projects reviewed on blockchain sharding [29] (© 2023 Springer Nature, reproduced with the permission of Springer Nature) (Continued)

Index	Domain	Consensus Protocol	Features (+ and -)
[36]	General	PoS	+ Used penalty mechanism to minimize the malicious nodes becoming leader of the shard. + Used probability distribution model to identify corrupt shards in the network. - Using PoS for shard leader selection, deprived the low stacks nodes to become a leader. - Using PoS for shard leader selection, deprived the low stacks nodes to become a leader.
[37]	IoT	PoW, PBFT	+ Deep reinforcement learning approach is used to select an optimal configuration of blockchain network. + DRL control of shards enhances throughput and security. -Fixed number of shards used in experiments i.e., 4 shards. - Increasing the number of shards decreases the security performance. Therefore, the system performs with a small number of shards.
[38]	General	PBFT	+ Presented a mechanism for choosing optimal shard size. + Identify faulty shards and discard all their transactions. - High inter-shard communication cost. - Detail of nodes assignment to shards is not provided

1.4.2 Blockchain Consensus

Blockchain, as a distributed ledger technology, has received extensive research attention in the healthcare domain for EHRs sharing among multiple CGs. Blockchain uses a consensus mechanism to ensure that all legitimate nodes reach an agreement to append blocks in the network. Various consensus algorithms have been reported in the literature for block validation and generation in healthcare. The consensus mechanism is the core of the blockchain technology, which started with Proof of Work (PoW), which has since been adopted by Bitcoin [1] and Ethereum [39].

An Ethereum-based healthcare blockchain framework was proposed in [40] using smart contracts for access control of medical data by applying cryptographic techniques for advanced security. However, the use of the PoW consensus algorithm in the above-mentioned framework consumes a significant amount of computational energy and time to reach consensus in the healthcare network.

A blockchain-based data preservation system [41] for medical data was implemented on the Ethereum platform using cryptographic algorithms to protect user privacy and medical data from tampering based on the PoW consensus algorithm. The primary limitation of this study was the lack of scalability owing to the complexity and energy consumption of the PoW algorithm. A blockchain IoT model was used in [42] to measure and collect a patient's real-time medical data using biosensors and storing data in the blockchain, ensuring a distributed network for patient medical status, billing information, and insurance coverage. A consensus was achieved using PoW algorithms among blockchain nodes; however, the computational cost and consensus time were the main hurdles. A patient location-sharing scheme was proposed in [43] for smart healthcare using blockchain technology. The mining process adopted a PoW mechanism, resulting in a gradual increase in the number of mining nodes as the network scaled up. However, no explicit mechanism was provided to deal with scalability in healthcare while running PoW consensus among several nodes.

To address the limitations of the PoW consensus algorithm, a growing number of consensus algorithms are being implemented in blockchain networks. Proof of Stake (PoS) has been used to address the problems of high-power consumption and computational time of PoW [44]. In PoS, the competition to solve a mathematical puzzle among miner nodes is eliminated, and miners that hold the highest stake in the network have the opportunity to mine a block. A blockchain-based framework for cross-domain medical image sharing using the PoS algorithm has been proposed [45]. In this framework, nodes must maintain a security deposit as a stake in the network to be selected as a miner. This raises the issue of forking because in a healthcare blockchain, keeping the security deposit is insufficient for the mining process.

Practical Byzantine Fault Tolerance (PBFT) algorithms are widely used in private blockchain platforms because they offer a practical solution to the high-power consumption and computational time of PoW and PoS consensus algorithms. Healthcare blockchain frameworks, including in [4, 21, 46], used PBFT consensus algorithms to gain a better performance than under Ethereum-based PoW algorithms. PBFT uses message exchange with all its peer nodes to reach a consensus in a five-step model. However, as

the network grows in size, the increasing number of messages exchanged degrades the consensus process.

PoA consensus algorithms are highly recommended and used in private blockchain networks to address this issue. PoA is a family of PBFT [47] wherein validating nodes are preselected in the blockchain network, resulting in fewer message exchanges and high performance. PoA algorithms are considered ideal for healthcare blockchain networks and have been used in recent works reported in [22, 48]. According to the literature, PoW algorithms consume the highest computational power of all consensus protocols, resulting in high consensus time, which can be a major problem in the healthcare domain because it may result in high risk to human life due to the time required for block generation. PoS consumes significantly lesser computational power and time than PoW; however, first, in the healthcare domain, preserving the stake is questionable; and second, the PoS algorithm guarantees that block rewards are restricted to stakeholders only, resulting in the poor becoming poorer and the rich becoming richer.

PBFT outperforms other existing algorithms. It requires each node to communicate with other nodes for message exchange to reach mutual agreement. However, in healthcare, as the number of nodes increases so does the number of messages exchanged, degrading the network performance.

EHRs sharing has revolutionized using blockchain technology in healthcare. It greatly facilitates the diagnosis of patients as their medical history can be used by various allied health professionals. Healthcare blockchain networks require an efficient and real-time consensus algorithm to improve the performance of the network in the shortest period. This study proposes an improved PoA consensus algorithm using instantaneous authority selection for each appointment. The proposed improved algorithm will select a minimal authority set yet provide an equal opportunity for all the healthcare entities to participate in the consensus process. Increasing the number of nodes in the network will not affect the performance of our proposed consensus algorithm.

1.4.3 Blockchains Interoperability

With the growing use of blockchain implementation in diverse domains, interoperability among isolated blockchains is an active research direction. In this context, interoperability

among blockchain networks is defined as the applicability of smart contracts between two independent blockchains [49]. In this section, we categorize the existing literature based on the various mechanisms used for inter-blockchain communication, including notary schemes, sidechain solutions, smart contract-based solutions, bridging solutions, industrial solutions, and hash time locks.

Notary schemes operate with a central trusted component that mediates the interaction between blockchain platforms and controls asset transfer. In such schemes, a single notary [50] or multiple decentralized notary solutions are used; in the latter case, a group of notaries from a consortium of notaries is used [51]. Various projects have employed notary schemes, including ICON [52], RIPPLE [53], Metronome [54], Interchain [55], and Cosmos [56].

Sidechains are secondary blockchains connected to the main chain and allow bidirectional data transfer between the two chains. This scheme is completely decentralized and uses pegged sidechains to lock and unlock assets in the chains during asset transfer. Sidechain schemes have been used in various projects for inter-blockchain communication, including RootStock(RSK) [57], Liquid [58], Elements [59], Pegged sidechains [60], Loom [61], and POA [62]. However, sidechain projects transfer assets in a one-to-one relationship among the same blockchain ledger.

Smart contract-based approaches use smart contracts to create inter-blockchain communication protocols among independent blockchain networks [63]. Schemes of this type provide decentralized and consistent atomic asset transfer among independent chains, where the changes are either committed or rolled back. However, these solutions are completely reliant on atomic swaps, which require the deployment of smart contracts on both blockchains. Projects that have adopted this scheme include those in [64 – 68].

Bridging solutions use smart contracts or other modules to operate as a bridge between two blockchain networks for data/asset exchange. They do not involve third-party mediators or any main chain for inter-blockchain communication, and they provide a decentralized model for communication. This scheme has been proposed in [69 – 72], but its implementation details are yet to be reported.

Blockchain router solutions are inspired by the role of routers in the Internet, and the first was deployed in 2017 [73]. In blockchain router architecture, different blockchains operate as sidechains but cannot communicate directly with each other; instead, the communication occurs via router nodes of each blockchain in the network. Models for the router approach have been provided in [73, 74, 75], but the implementation details of router node architecture still need further investigation.

Although blockchain technology has revolutionized the healthcare industry, several healthcare blockchains still operate in silos, and research is in progress to create cross-chain communication protocols to share EHR across homogeneous and heterogeneous networks. AppXchain [76] is an application-based cross-chain interoperability model that integrates independent blockchains for EHR sharing. However, the proposed model uses only Ethereum-based networks and is not yet applicable to other blockchain platforms.

In this section, various solutions for inter-blockchain communications for homogenous and heterogeneous blockchains and their limitations are analyzed. A summary is presented in Table 2. Sidechain solutions are widely adopted in literature. However, the major drawback of techniques using sidechains is the one-to-one communication among homogeneous blockchains. Furthermore, in the implementation of a sidechain, security vulnerabilities in the blockchain federation increase when a sidechain in the network is compromised. Blockchain routers provide connectivity solutions for heterogeneous blockchain networks, but none have been implemented yet. Moreover, such implementations require the architecture of the router nodes to be configured to function as routers. Another limitation of the blockchain router technique is the single point of failure issue: When any router node fails, communication among any participating networks is compromised.

The healthcare domain is a highly in-demand field that requires solutions for inter-blockchain communication in a blockchain federation. However, this area of research has not been fully explored, and further investigations are needed. Therefore, this research proposes a novel “transaction-based inter-blockchain communication” technique based on global and local smart contracts in a healthcare federation to address the interoperability challenges among independent blockchains.

Table 2: Summary of the projects reviewed for inter-blockchain communication solutions.

Index	Consensus	Features (+ and -)	Solution Type	Shortcomings of the Solution
[57]	PoW	+ Work as sidechain pegged to bitcoin. + Faster validation of transactions. +Less transaction fee. - Cannot operate independently, completely depends on bitcoin main chain.	Sidechain solution	Supports 1-1 communication among sidechains and main chain. Focus on homogenous blockchains. Higher computational cost and complex. Sidechain blockchains cannot operate independently
[77]	PoS	+ Each sidechain has its own independent rules and constraints. - Mining is performed on the main chain. - Completely dependent on the mainchain for the mining process.		
[65]	Heterogeneous Consensus	+ Sidechains use independent consensus algorithms. + Maintain private ledger which provides faster blocks generation. - Private ledger is not shared with all the participants.		
[78]		+ Uses a federated two-way peg mechanism. +Provide increased security to the funds transfer among sidechains and main chain. - The federated two-way peg mechanism increases the transactions validation time.		
[73]	Delegated Stake PBFT	+Provided communication among heterogeneous blockchains. +Can add blockchain routers dynamically. - Communication via blockchain router only. -One point Failure issue can compromise communication.	Blockchain router solution	Design and frameworks are available but are not implemented yet. The configuration of the blockchain node needs to be changed to function as a router node. One point failure issue. Communication is affected as the router node fails or is compromised.
[79]	PBFT	+Different Blockchain systems communicate without any intermediaries. +Using Ann-Router-based network architecture, a part of blockchain function as a router, however, configuration details of such setup is required. - The connection mechanism is not provided. -Based on each blockchain topology, throughput is affected. -Implementation details are missing.		
[74]		+Created a dynamic blockchain network called router blockchain, which included router nodes from each blockchain. - One point failure issue due to communication via a single node. -The configuration setting of the router node is not provided.		

Table 2: Summary of the projects reviewed for inter-blockchain communication solutions. (Continued)

Index	Consensus	Features (+ and -)	Solution Type	Shortcomings of the Solution
[64]	PoS	+ Smart contract-based interoperability solution between independent blockchains (public and private) without intermediaries. -The authors didn't apply their solution between two-hybrid systems.	Smart contract solutions	Available solutions operate in homogeneous blockchains. Smart contract solutions are in infancy and implementations are not available. Smart contract sharing is not available.
[50]		+Cross-blockchain data transfer, smart contract interaction, currency transfer. +Transfer the same kind of token to any number of blockchains simultaneously. -The proposed protocol operates in the same environment only, among homogeneous blockchains.		
[66]		+A cross-chain atomic swap is used for transferring or exchanging assets between multiple participants across multiple Ethereum blockchains. -Need to implement atomic swaps on and with other blockchains.		

Chapter 2: Methods and Results

This section presents a comprehensive methodology for accomplishing the four objectives that form the foundation of this research. The methodology is divided into four sections, each dedicated to one of the research objectives. As the techniques and frameworks employed to analyze the results vary across objectives, individual subsections are included to outline the proposed models for each objective, present the obtained results and outcomes, and provide a thorough discussion of the findings.

2.1 Methodology

The high-level overview of the proposed method to address the main objectives of the study is illustrated in Figure 1. We propose blockchain federations for EHRs sharing using a global smart contract methodology; address the scalability issue in the individual blockchains of a federation using the sharding technique; and propose an improved PoA consensus algorithm using instantaneous authority selection in the healthcare domain.

A patient Pi visits a CG in blockchain B1, who has their EHRs in blockchain B2. At the beginning of the appointment, CG creates a transaction proposal for Pi, specifying the transaction type as “inter-blockchain/intra-blockchain.” The transaction type is used to trigger B1’s local and global smart contracts. The transaction type “intra-blockchain” triggers B1’s local smart contract to access the patient record of B1 nodes. An “inter-blockchain” type transaction, on the other hand, triggers B1’s global smart contract to establish a communication link to B2 to access Pi’s EHRs from B2 nodes. The details of the proposed techniques to address each objective are presented in the following sections.

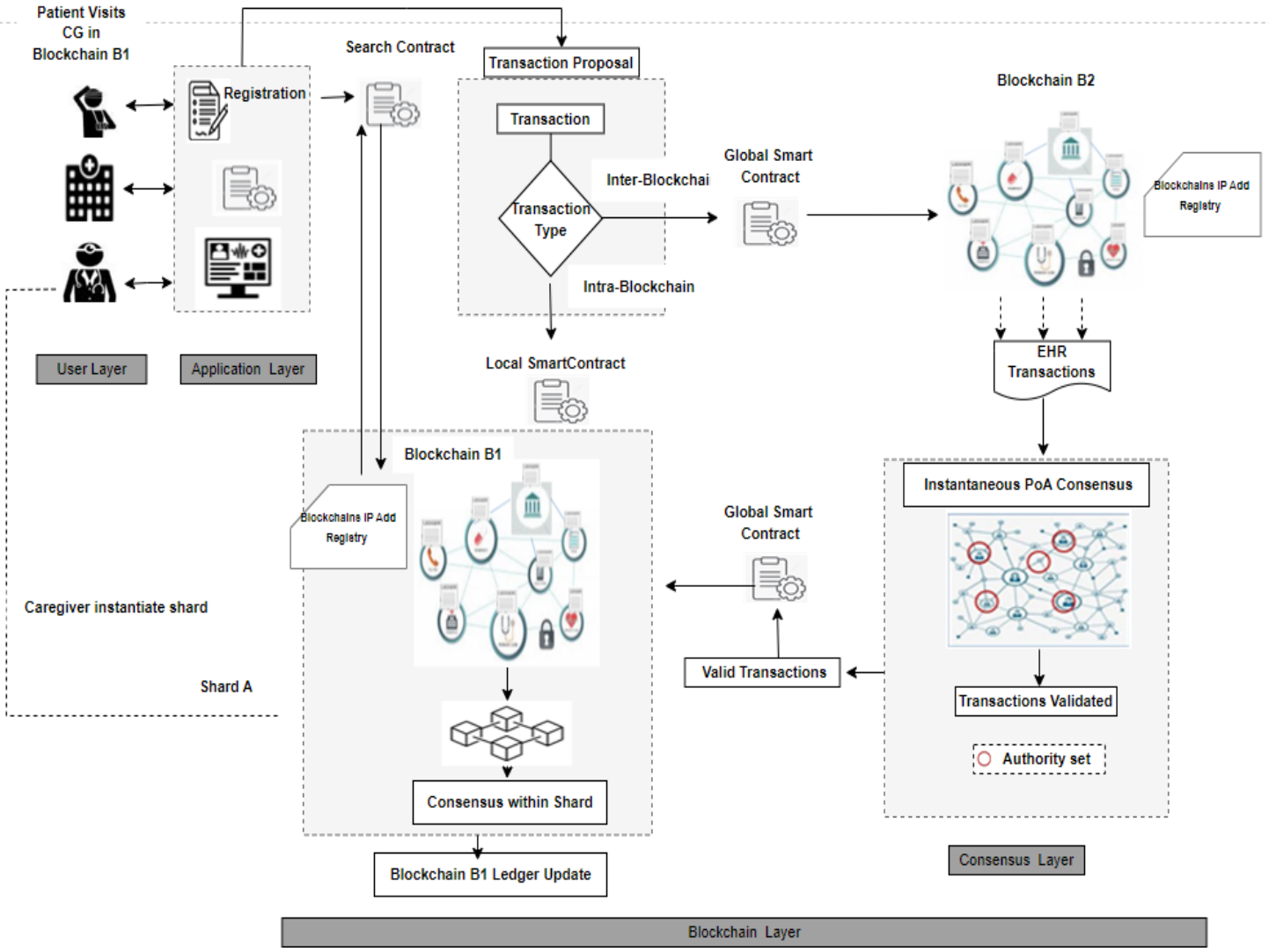


Figure 1: Proposed blockchain federation for EHRs sharing.

2.2 Scaling up Healthcare Blockchain using Sharding

One of the major challenges in blockchain is scalability issues. The sharding technique has been used successfully in many domains for scalable blockchain development [24, 25, 26, 30, 31, 33, 80, 81]. However, resolving the scalability issue using sharding has an overhead of cross-shard communication, where a node in one shard needs to communicate with the nodes in another shard. Cross-shard communication overhead is more complex, which makes the verification process more challenging [66].

The proposed sharding technique in healthcare uses a "transaction-based shard formation" technique to minimize the network overhead. The shards are formed based on the presence of patients' records in the participating nodes with access permission from the patients. As a result, the proposed technique forms complete shards for an appointment. Therefore, the shard nodes do not need to communicate with nodes in other shards, eliminating the cross-shard communication overhead. During the appointment between a CG and a patient, any record can be requested through transactions within the shard only. Figure 2 shows the proposed architecture for a sharded blockchain-based healthcare data-sharing system.

Shard formation is an important task in a sharded blockchain network. Various clustering algorithms are used for shard formation in the literature, including peer discovering algorithms, user assignment algorithms, smart contract-based shard formation, demographic clustering algorithms, and nearest neighbor algorithms. Initially, these algorithms exhibited good performance in shard formation, but they were unable to make the process efficient because they increased the cross-shard communication overhead. According to one study [81], 95% of the communication in a sharded blockchain is performed as a cross shard, which degrades the network TP.

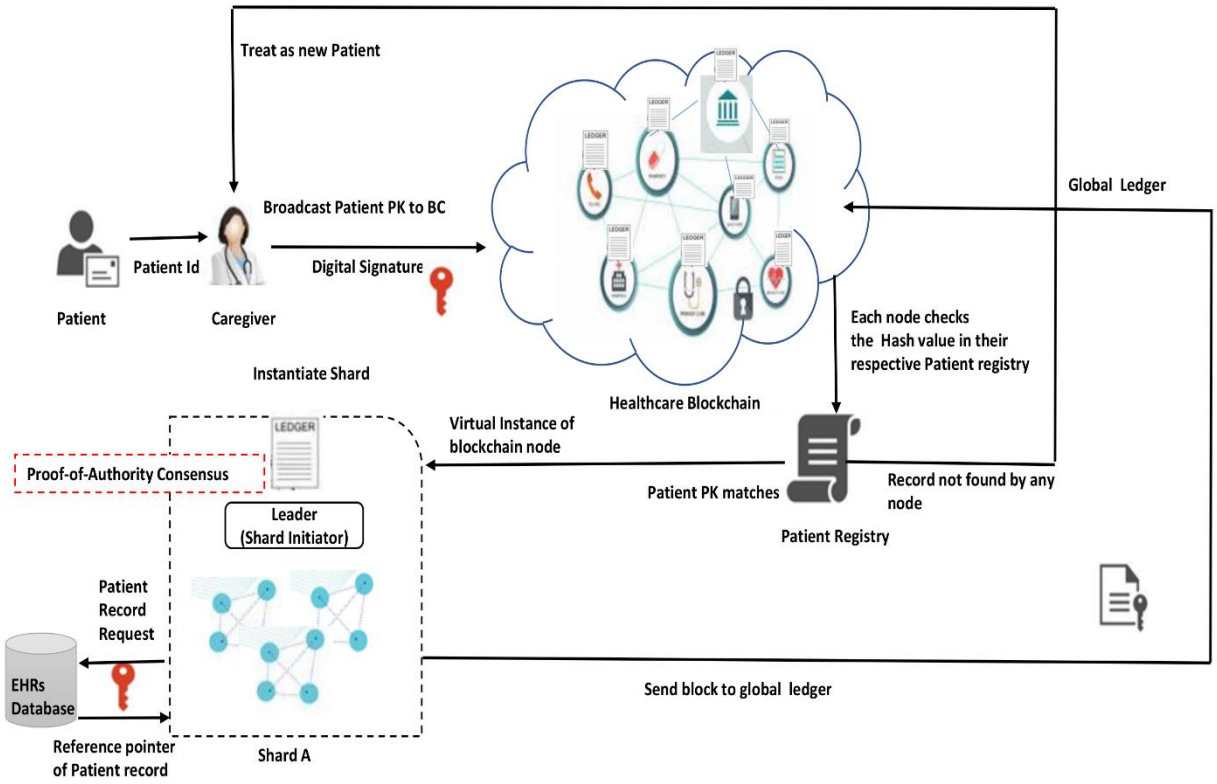


Figure 2: Proposed sharded blockchain-based EHRs sharing system workflow.

This study eradicates cross-shard transactions to increase network TP by using "transaction-based sharding," such that shards are formed based on patients' records present in the corresponding nodes. This process results in smart shard formation and eliminates cross-shard communication since all the nodes previously visited by the patient are grouped within the same shard. Each appointment in the network is processed in the shard. Thus, the number of shards formed in the healthcare blockchain network is directly proportional to the number of active patient appointments in the network. Forming permanent shards may result in a large number of active appointments, which may lead to low TP. Thus, in our proposed model shards are discontinued at the end of a patient's appointment/service with the CG who initiated their creation. Hence, the resources of other participating nodes are released, and there is no TP degradation within the network.

2.2.1 Performance Evaluation

Scalability is a major concern in any fast-growing technology. In the case of blockchain networks, scalability is defined in terms of TP, LT, storage, and block size. This section analyzes the proposed scheme using a performance matrix in a blockchain network, such

as TP, consensus LT, and number of transactions processed for each appointment. The analysis compares the proposed sharding technique with the unsharded techniques used in healthcare blockchain.

Consensus Latency: LT refers to the delay between the time a transaction is added in a block by a consensus participant and that when the block is validated by a majority of the consensus nodes. As the number of transactions increases in the blockchain, the verification and confirmation time of transactions increases rapidly. The proposed sharded blockchain runs a PoA consensus among the shard nodes locally with S_N number of nodes (where $S_N \subset B_N$); therefore, the waiting time for the verification of a transaction is minimized by the careful choice of the number of verifiers within the shard. Our scheme eliminates the leader selection step as the shard initiator is appointed as the leader of the shard. We analyze the consensus LT of each appointment. Let T_c be the confirmation time and T_s the submission time of the transaction for consensus, respectively, with a round trip network delay. Then, the consensus LT $u_{nshaded}$ per shard is represented by Equation (1), which is used for the calculation of LT in our proposed blockchain network.

$$L_T = T_c - T_s \quad (1)$$

Where T_c of valid transactions depends on the consensus time, T_{cons}, during message exchanges among validator nodes and the shard leader node, then

$$T_c = T_{cons}$$

Then, consensus time is calculated by

$$T_{cons} = \text{Max}\ (T_{(L,V)}) + \text{Max}\ (T_{v1}, T_{v2}, T_{v3} \ldots T_{vn}) + Max\ (T_{(V,L)}) \quad (2)$$

Where $T_{(L,V)}$ represents the Communication Time (CT) for sending a block from the leader node to the validator nodes; we consider the maximum time from this set. (T_{v1}, T_{v2}, $T_{v3} \ldots T_{vn}$) represents the CT of sending the block from each validator to every other validator within the shard. In equation (2), T_{v1} is the CT of validator V1 to every other validator such that V1 = Max (T_{V12}, T_{V13}, $T_{V14} \ldots\ldots TV_{1n}$). $T_{(V,L)}$ represents the CT of sending the commit from validators to the leader node.

Throughput: Blockchain TP is defined as successful transactions per second given a particular network size. Transaction LT and TP are inversely proportional to each other as

the confirmation in a blockchain depends on the consensus mechanism. Considering an unsharded blockchain network processing T_c number of transactions per second, as the transactions are broadcast to all nodes in the network, B_N, the TP drops as time evolves. In the proposed scheme the entire network is divided into *K* shards, where *K* depends on the number of active appointments in the healthcare consortium model. Each shard processes a distinct set of transactions; therefore, as the number of transactions increases in the network, the transactions are processed in parallel within the shards. Thus, all transactions are processed in the shards within a unit time, and the overall network capacity to process transactions improves. If CT_{xn} is the total transactions confirmed, PT is the total processing time, and ST_{xn} is the transactions confirmed within the shard, then

$$TP = \left(\frac{CT_{xn}}{PT+ND}\right) \quad (3)$$

Where,

$PT = T_{app\_end} - T_{app\_start}$

Such that

T_{app_start} = Appointment start time

T_{app_end} = Appointment end time

Then

$PT = [Max(T_{(SN)}) + T_{cons} + T_{L\_confirm}] - T_{app\_start}$

Where $T_{(SN)}$ represents the CT of sending transactions by shard nodes, T_{cons} represents the CT of consensus process, and $T_{L\_confirm}$ represents the confirmation time of the block by the leader after receiving n/2 +1 commit messages from validator nodes.

From eq(2)

$PT = [Max(T_{(SN)}) + [\text{Max}(T_{(L,V)}) + \text{Max}(T_{v1}, T_{v2}, T_{v3} \ldots T_{vn}) + Max(T_{(V,L)}] + T_{L\_confirm}] - T_{app\_start}$ (4)

$CT_{xn} = \sum_{i=1}^{k}(S_i T_{xn(i)})$ (5)

Where $S_i\, T_{xn}$ represents the transactions confirmed by shard S_k. Then, using Equations (4) and (5), TP can be calculated as:

$$\text{TP} = \frac{\sum_{i=1}^{k}(S_i T_{xn(i)})}{PT+ND}$$

Hence, adding the confirmed transactions in each shard will increase the TP of our proposed technique. Increasing the number of appointments will result in an increased TP of the proposed network.

2.2.2 Results and Discussion

In this study blockchain sharding in the healthcare domain for EHRs sharing is evaluated and compared with an unsharded network. The experiments were performed by simulating the proposed sharded and unsharded healthcare blockchain using Python 3.6 on a Windows 10, Intel(R)® Core(TM) i5-8256U CPU, 64-bit operating system. The CG nodes are the authorized blockchain nodes and participate in the consensus step to validate the transactions for each appointment. In this setup, the appointment follows a Poisson distribution, such that each appointment arrives at an arbitrary positive time. We simulated a minimum of 50 CG nodes and examined the scalability of the network by increasing the number to 100, 150, 200, and 250. A block size of 1 MB was used, which consists of transactions for each appointment. A block in blockchain is comprised of a header and the body. The block header includes the metadata information (previous block's hash value, Merkle root hash value, block number, and timestamp), and the body part of the block includes the transactions related to the patient's EHR. SHA 256 was used as a hashing algorithm in our experiments. For each appointment a random number of shard sizes was generated in the range of 2 to 20. The shard size implies the number of CGs previously visited by the patient; therefore, we used a random shard size for each patient.

To summarize the obtained results from the various simulated scenarios, we examined the impact of our proposed sharding technique on the performance of a healthcare blockchain and compared the results against the unsharded model. The performance of the proposed sharded-based model was examined in terms of the number of appointments processed, consensus LT, and TP. The results demonstrated a significant increase in appointment processing in shard-based healthcare as compared to the unsharded network. Our proposed technique processed appointments in parallel within shards, resulting in low LT and high TP, as shown in Figure 3 and Figure 4, respectively.

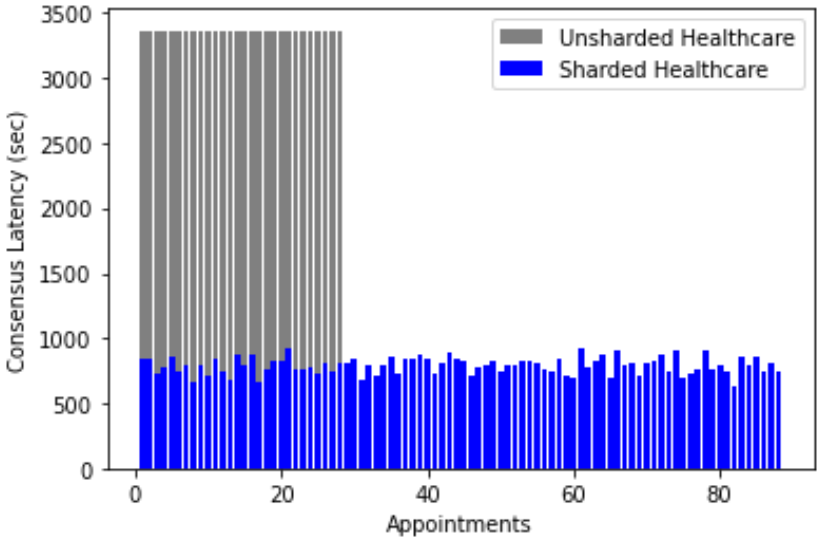


Figure 3: LT of proposed sharded and unsharded healthcare blockchains.

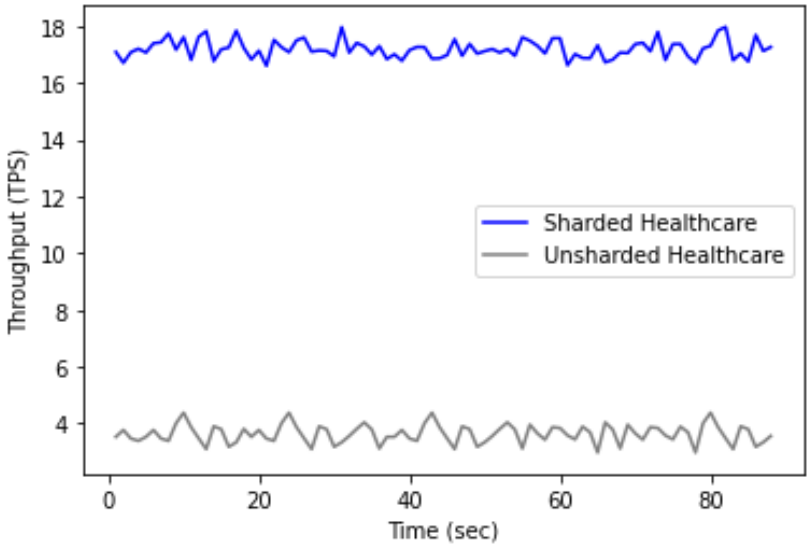


Figure 4: Throughput of the proposed sharded and unsharded healthcare blockchains.

Next, we analyzed the scalability of our proposed technique when the number of blockchain nodes was increased. The obtained results showed that our proposed model is more scalable than unsharded network as increasing the number of nodes had no significant impact on the performance since transactions were processed within each shard with the minimal number of shard nodes participating in the consensus process.

Redrafted from: Hashim, F., Shuaib, K. and Sallabi, F., 2021. Medshard: Electronic health record sharing using blockchain sharding. *Sustainability*, *13*(11), p.5889.
This research work is based in [full or part] on the previously published article listed above. I have permission from my co-authors/publishers to use the work listed above in my thesis/dissertation.

2.3 Improved PoA Consensus using Instantaneous Authorities Selection

In blockchain technology, consensus is a mechanism implemented to arrive at a common agreement in a decentralized network. In the absence of any central authority, consensus protocols are used to monitor all transactions and maintain a single view of shared data in the global ledger of the blockchain. In this study, we propose an improved PoA consensus algorithm using instantaneous authority selection for EHRs sharing in healthcare. In PoA consensus, authorities are honest nodes that must participate in the consensus process for block validation [22, 82], with an agreement among a minimum of (n/2 + 1) authorities. The number of authorities in a consensus process is inversely proportional to the number of blocks validated and generated in the blockchain. Hence, the selection of authorities is crucial in the consensus process.

The authors in [83] select full nodes in the network as authorities. This process filters honest nodes in the network; however, in the healthcare domain the number of full nodes increases as more nodes are registered in the network. In [84] the proposed approach works with a predefined set of authorities in a network; however, the selection criteria of authorities are not provided. In this case, not all honest nodes will have the opportunity to participate in the validation process. Considering these limitations of PoA authority selection, we propose an instantaneous authority selection, providing an equal chance to all full nodes in a healthcare network to be a candidate for authority selection while maintaining a minimal set of authorities.

In the proposed methodology, as shown in Figure 5, CGs previously visited by the patient provide the EHR of the patient under observation upon the request of the current CG. The transaction generated by each provider includes the provider's and the patient's public keys along with the patient's previous record. The transaction data are hashed using SHA 256 [85]. Once all the transactions are added to a transaction pool, the proposed consensus

algorithm selects the authorities based on the public key of the allied health professionals in that pool, implying that the nodes that provide EHR data will participate in the consensus process. In this method, CGs previously visited by a patient serve as validators for the patient's appointment, yielding a filtered set from the network's honest authorities. This instant selection of authorities for each appointment reduces the number of validators in the consensus process; thus, with fewer messages exchanged, the consensus time is significantly reduced in the healthcare domain.

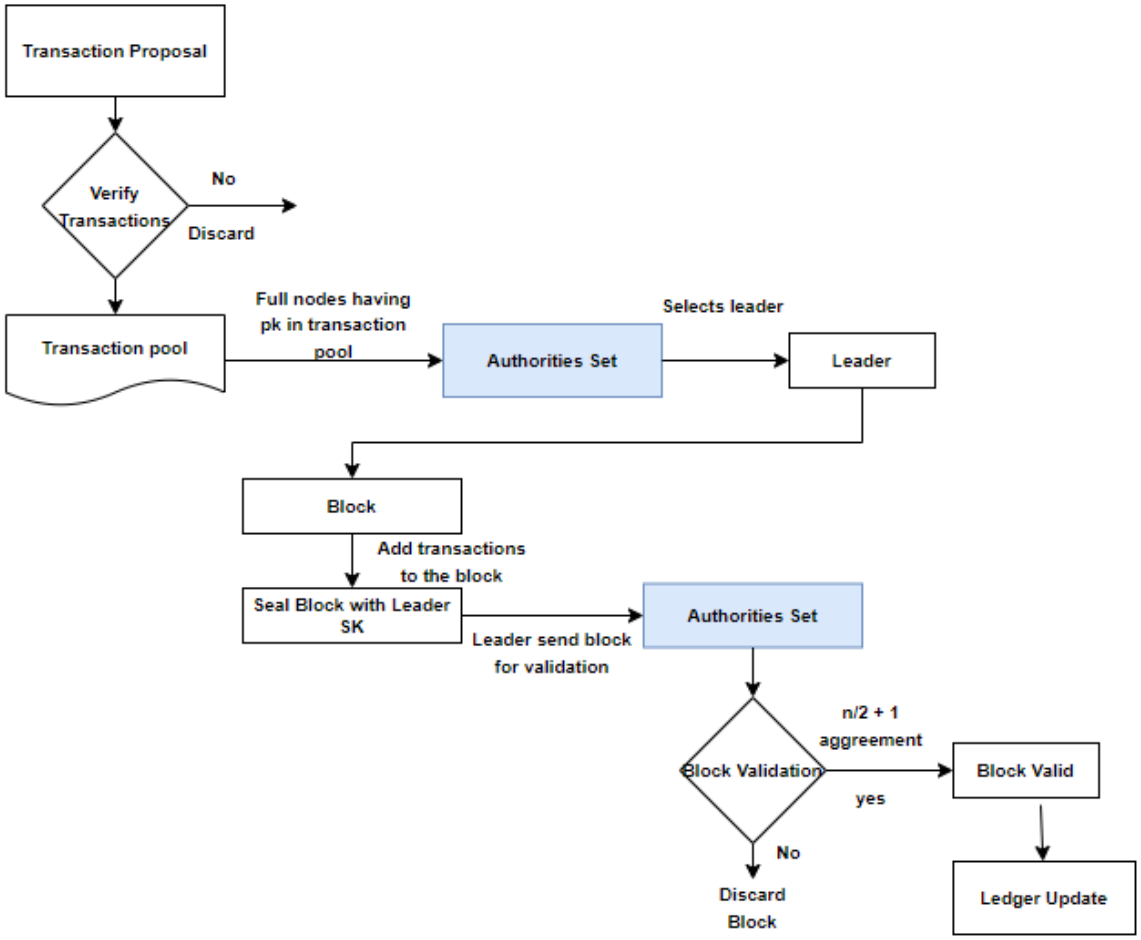


Figure 5: Workflow of the proposed improved PoA consensus algorithm for EHR sharing (©2021 IEEE).

2.3.1 Results and Discussion

We evaluated the performance of blockchain consensus algorithms, including PoW, PBFT, PoA (Aura) [86], PoA (Apla) [87], and our proposed PoA in the healthcare domain for EHR sharing using TP and LT performance measures.

One hundred healthcare blockchain nodes were simulated, including allied health professionals, hospitals, insurance companies, and pharmacies, to provide the EHRs of visiting patients. Each appointment in the network generated a block comprising a single patient's record, shared by previously visited allied health professionals. The performance was evaluated in terms of the consensus time, number of blocks generated, and network TP. The experimental results showed a significant increase in TP and decrease in consensus time of our proposed PoA consensus algorithms as compared to previous solutions, as shown in Figure 6 and Figure 7, respectively.

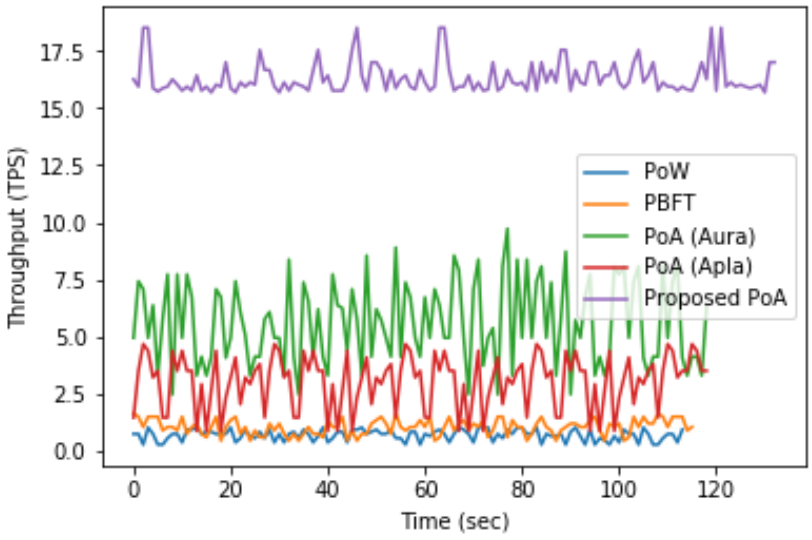


Figure 6: Blockchain consensus algorithms throughput comparison in healthcare.

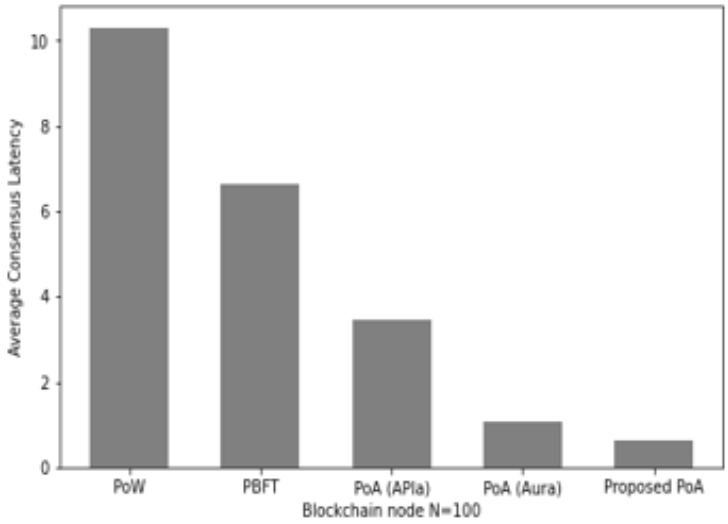


Figure 7: Blockchain consensus algorithms consensus time comparison in healthcare.

Then, we tested the scalability performance of different consensus algorithms with an increasing number of nodes in a healthcare blockchain network. PoW is considered scalable because the consensus process depends on solving the computational puzzle by miners; thus, it is independent of the number of nodes. However, the consensus time of PoW depends on the difficulty level of the computational puzzle. Therefore, we performed the scalability test with PBFT, PoA (Aura), PoA (Apla), and our proposed PoA. We increased the number of nodes from 100 to 200, 300, and 400 and analyzed the effect of increasing the number of nodes on the different consensus algorithms.

Summarizing the results, the scalability test results showed that our proposed PoA algorithm outperforms the other compared algorithms, indicating that it is a highly scalable algorithm and thus a better candidate for the healthcare blockchain domain.

Redrafted from: Hashim, F., Shuaib, K. and Sallabi, F., 2021, December. Performance Evaluation of Blockchain Consensus Algorithms for Electronic Health Record Sharing. In *2021 Global Congress on Electrical Engineering (GC-ElecEng)* (pp. 136-143). IEEE.

This research work is based in [full or part] on the previously published article listed above. I have permission from my co-authors/publishers to use the work listed above in my thesis/dissertation.

2.4 Blockchains Federation for Interoperability in Healthcare

Blockchains are immutable distributed ledger systems that provide trustable qualities such as security, decentralization, integrity, safety, and connectivity without the need for a central authority [1]. Blockchains and other distributed ledger technologies have gained much attention from industry and academia, and the use of blockchain technology to ensure data integrity between entities has been shown to be beneficial. Blockchain technology has demonstrated its versatility in recent years as various application domains have sought methods to incorporate its capabilities into their operations. Although this technology has been particularly investigated by the financial services industry to date, efforts in other service-related fields, including healthcare, suggest that interest in it is broadening. Indeed, the literature now contains multiple studies of the use of blockchain technology in the healthcare sector, including [11, 18, 21, 35, 46, 48, 88 – 91]. Because of healthcare privacy and security concerns, private or consortium models are adopted in healthcare blockchains; however, most blockchains are currently designed as silos without the ability to interact. The resulting serious inefficiency needs to be addressed so users can use and share their digital assets/data across multiple independent blockchain networks efficiently.

Blockchain interoperability has emerged as an active research topic for sharing data/assets among different blockchain networks. This area of research is still largely theoretical; however, many projects have attempted to devise a practical solution in a one-to-one relationship. In this section, we propose a blockchain federation to address the blockchain network integration challenges. The proposed high-level overview of the blockchain federation is shown in Figure 8.

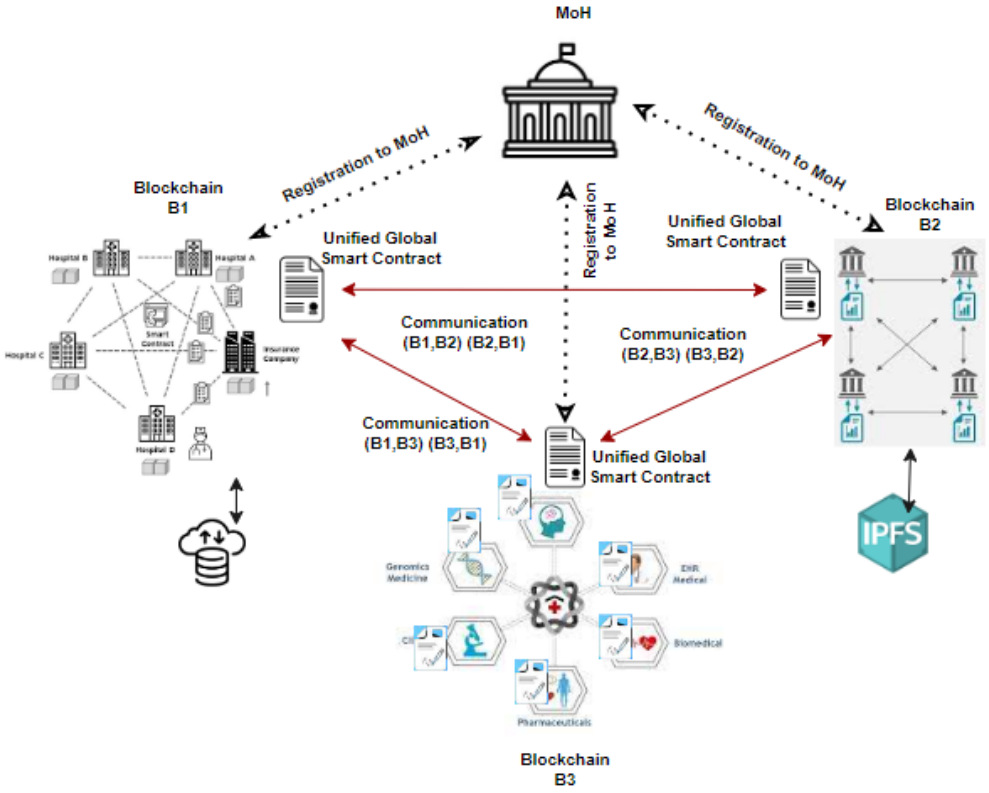


Figure 8: Proposed blockchain federation overview.

The proposed federation consists of multiple healthcare blockchains deployed via the same and different platforms. Each network functions independently following a distinct business logic, data storage mechanisms (i.e., interplanetary file system (IPFS) or cloud-based), smart contracts, and validation process. In the proposed federation, each network requires prior registration to a central unit, that is, a Ministry of Health (MoH). This one-time registration occurs during the first deployment to receive the blockchain ID from the MoH. The interoperability mechanism in the federation follows the following assumptions:

- The individual blockchain networks function independently but are registered in the federation with a blockchain ID.
- Each blockchain network has a repository of blockchain addresses registered in the federation.
- The interoperability solution may request data from another blockchain but cannot make any changes to the state of the connected network.

- The communicating networks are unaware of the target network's architecture; therefore, each network deploys a unified module to accept transactions from other networks.
- The interoperability mechanism cannot directly trigger the smart contracts of another network.

The blockchain network is a distributed ledger technology that functions without any central entity. The proposed blockchain federation maintains the decentralization of the networks in a federation. However, the presence and function of the central unit (MoH) provide for the communication process among the independent networks. The central unit does not interfere in the communication process among the blockchains. A step-by-step registration process is provided in Algorithm 1:

Algorithm 1 Blockchains registration in a federation

1: $Input : Blockchains(B1, B2, B3, ...Bn)$
2: $Output : R\_B\_list$(Registered Blockchains List)
3: $Root\_CA_{B1} \rightarrow$ registration request
4: MoH authenticate $Root\_CA_{B1}$ request
5: **if** authentication = true **then**
6: $registeration \rightarrow successful$
7: MoH assign id to $Root\_CA_{B1}$
8: MoH send Unified_Components to $Root\_CA_{B1}$
9: **if** $Unified\_Components$ implemented in B1 **then**
10: MoH add $Root\_CA_{B1}$ address to R_B_list
11: **else**
12: $AbbortSession$
13: **end if**
14: **end if**
15: $R\_B\_list \rightarrow update$
16: MoH send R_B_list update to $B_n infederation$
=0

Within a federation, multiple independent blockchain networks exist that might be deployed via different platforms. In this case, interoperability happens between the same platform networks (homogeneous) or between different blockchain network platforms (heterogenous). The proposed inter-blockchain communication of homogeneous and heterogeneous networks is discussed in the following section.

2.5 Homogeneous Blockchains Integration for EHRs Sharing in a Federation

This section proposes a transaction-based smart contract triggering technique in inter-blockchain communication for EHR sharing among independent homogeneous blockchains, as shown in Figure 9. In this setup, each blockchain holds a unique blockchain ID (e.g., B1, B2, B3, B4) that is preregistered with an overarching entity, such as an MoH. Our system consists of several nodes that can take any of the following roles: hospitals, that are full nodes for executing transactions (requesting and granting access to a patient record); patients, who can only view their medical record; allied health professionals, who can request patients' EHR; validators, who participate in the consensus process; and regulators, who enforce policies and handle registration of nodes to establish connections (e.g., the Certification Authority (CA) for each blockchain) without necessarily participating in the consensus process.

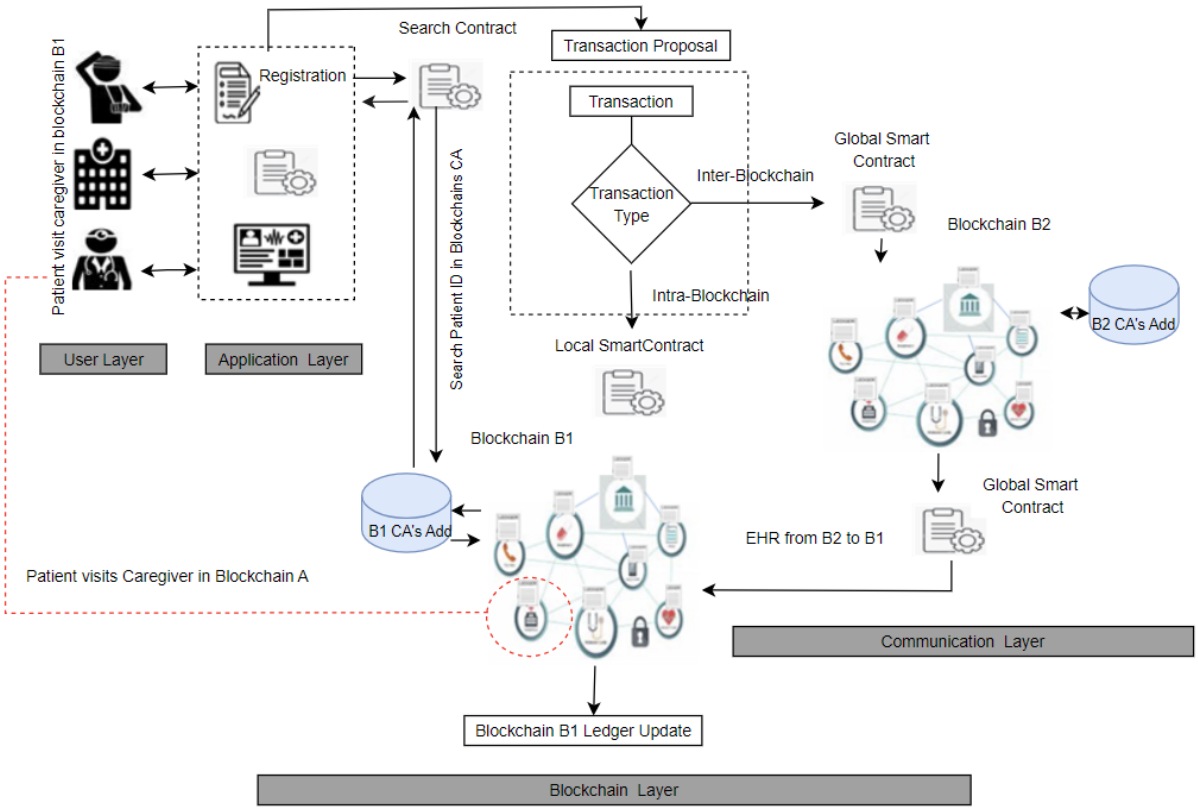


Figure 9: Proposed homogeneous blockchain integration model for EHR sharing.

The proposed architecture consists of four layers: user, application, blockchain, and communication. The user layer consists of clients who interact with the blockchain network using a decentralized application, where each node will conduct transactions directly with its peers in the network. The application layer monitors the registration process of the participants in the blockchain and generates the encryption keys of registered users. In this architecture, the application layer triggers a search contract after a patient is registered to search for their record in other blockchains of the federation. The blockchain layer comprises the network's core components, including network participants, consensus mechanism, and smart contracts. The communication layer uses global smart contracts to create communication links to other blockchains for data sharing in a blockchain federation.

Smart contracts play a vital role in blockchain operations. Smart contracts are programmable modules stored on a blockchain that are triggered when predetermined conditions are met. They can also automate a workflow, triggering the next action when conditions are met. Smart contracts automate the execution of a condition or an agreement so that all network nodes can be promptly advised of the outcome without the involvement of any mediators. The proposed blockchain layer entails four types of smart contract: search, global smart contract, local smart contract, and data contract.

The search contract is triggered at the application layer after the patient is registered in the blockchain network. The functionality of this contract involves searching for a patient ID in the CA address registry to identify the blockchain in which their EHRs exist. The input in this contract is the patient ID, as this is identical in all blockchains within the federation. The global smart contract is triggered at the communication layer when the transaction type in the transaction proposal prepared by the current CG is identified as "inter-blockchain". This contract allows communication among independent blockchains in a federation to share the EHR of patients under observation. The local smart contract is triggered when the transaction type to access a patient's EHR within the same blockchain being currently visited by the patient is "intra-blockchain." The data contract provides CGs with the functionality to add data to the blockchain. The EHR of patients are stored in IPFS, and the hash of these records is stored in a data contract that can be easily accessed by authorized nodes.

2.5.1 Results and Discussion

In this section, we conducted several experiments to individually evaluate the performance of both blockchains (B1 and B2) and then evaluate the average response time of query transactions from blockchain B1 to B2. The proposed model evaluation was performed through evaluation metrics including TP, transaction LT, CPU utilization, and average Elapsed Time (ET). The scalability of blockchain networks was evaluated to analyze the platform's ability to support the increasing transaction load, including the increasing number of nodes on the network. It indicates the acceptability of the network performance while varying the number of nodes and transaction load.

The blockchain-based framework Hyper Ledger Fabric (HLF) [92] was used to develop two independent private blockchain consortiums for efficient data sharing in healthcare, where several health entities form a peer-to-peer consortium network. HLF is a scalable blockchain platform that is widely used in a variety of contexts, including healthcare [93], IoT traceability [94], self-sovereign identity [95], digital couponing [96], and supply chain management [97]. HLF is an open-source permission-based distributed ledger technology, where all the participants know each other. Therefore, the network is fully trusted and secure.

The main contribution of this research is the integration of independent blockchains in a healthcare federation. To accomplish this, two independent blockchains (B1 and B2) were developed using the above configuration. Different networks have different numbers of entities in a federation, based on their requirements. To develop the test networks, we started with a minimum number of healthcare entities owing to the limited CPU power of our system. However, we used a different number of healthcare entities in the two blockchains to track the performance of both networks with a different number of nodes. B1 comprises three healthcare entities (hospital-A, hospital-B, and hospital-C). Each healthcare entity has at least two peers (peer0 and peer1), one orderer, a CA, and a peer node as an endorser in the network. Blockchain 2 consists of four healthcare entities (hospital-1, hospital-2, hospital-3, and hospital-4) with the same settings as blockchain B1. Both blockchains executed transactions independently in the testbed environment and used CouchBD as the state database deployed on each peer node.

Average ET measures the average ET for query transactions from one blockchain network to another, that is, from blockchain B1 to B2. For example, B1's ET can be calculated from the start time (T_s) of a client request initiated by B1 to the time the client received the response from B2 (T_R), such that

$ET = T_R - T_s$

In the communication process, the ET depends on the query processing time (QT) by

B2's round-trip CT from B1 to B2. Hence,

$ET = CT + QT_{B2}$

The QT at blockchain B2 can be calculated as follows:

$QT_{B2} = RT_{B2} - QT_s$

where RT_{B2} represents the response time for the query by B2, and QT_s represents the query start time in B2. Then, B1 ET can be calculated as follows:

$ET = (RT_{B2} - QT_s) + CT.$

The detailed results are provided in Article 2. Summarizing the inter-blockchain communication results, the average ET was calculated for a query transaction from B1 to B2. The ET for the first query transaction was very high because of the initial connection to blockchain B2. After the connection was created, a gradual drop in ET for the second client request and onwards was recorded, as shown in Figure 10. The query processing time at B2 was also evaluated, and it was concluded that the ET at B1 depends on the query processing time at B2.

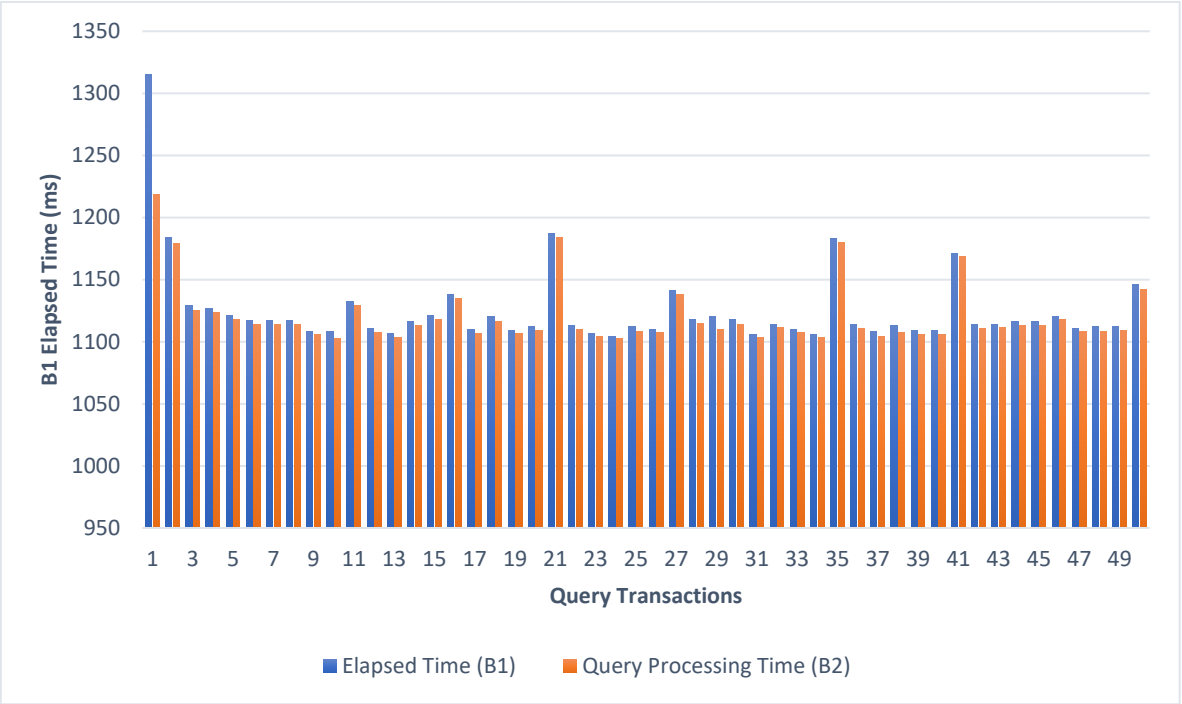


Figure 10: B1 ET vs. B2 query processing.

We compared the latency of our proposed approach for transferring EHRs between blockchains with a solution previously reported in [56]. The paper used a trusted execution environment for asset transfers among blockchains in a supply chain domain. We compared our results with the work of the supply chain management domain, as the results of inter-blockchain communication implementation are extremely limited to date. Specifically, our work constitutes the first example of implementation in the healthcare domain, to the best of our knowledge. Therefore, we looked at the available literature results from other domains for comparison. The results showed that our proposed transaction-based inter-blockchain communication technique significantly reduced latency for inter-blockchain transfer over the previous solution, as shown in Figure 11.

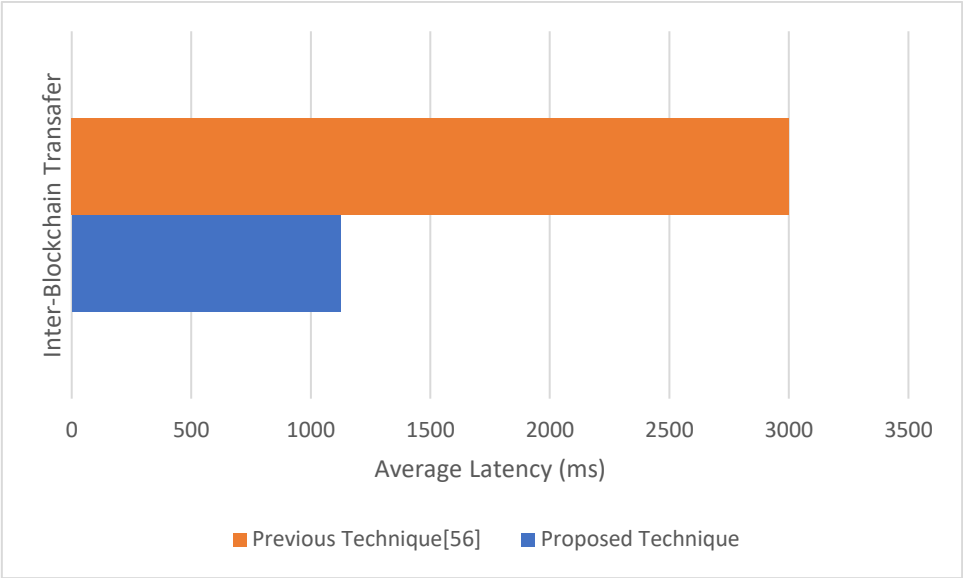


Figure 11: Comparison of average latency in inter-blockchain communication.

Redrafted from: Hashim, F., Shuaib, K. and Sallabi, F., 2022. Connected Blockchain Federations for Sharing Electronic Health Records. *Cryptography*, *6*(3), pp.47.
This research work is based in [full or part] on the previously published article listed above. I have permission from my co-authors/publishers to use the work listed above in my thesis/dissertation.

2.6 Integration of Heterogeneous Blockchains to Share EHRs

Blockchain interoperability can result in a paradigm shift of an open system in which devices and users can interact with each other across blockchain boundaries to meet the demands of complex decentralized applications. However, existing inter-blockchain communication protocols are limited to homogeneous blockchain platforms such as Ethereum-based blockchains and do not support interoperability between heterogeneous blockchain platforms. This makes it difficult to carry out transactions across diverse platforms of blockchain networks, which might have significant implications. For example, a patient's record residing in one blockchain platform might not be accessed by another blockchain running a different platform in timely fashion when needed. Currently, there are no layer-1 blockchain protocols that can carry out (i) transactions on another blockchain and (ii) smart contract invocation and interaction across blockchains [98].

In the current research, we consider a blockchain federation [99] that consists of diverse blockchain networks deployed via different platforms (i.e., HLF and Ethereum). We deem heterogeneous blockchains to be those that are deployed on different platforms and have a distinct business logic and design. In this type of blockchain system, while working with one platform it is not possible to make a direct transaction to another platform because of architectural and functional differences. Therefore, we propose a cross-chain communication protocol to carry out transactions among the heterogeneous blockchains in a federation.

In this study, we propose a global smart contract-based triggering solution for communication among heterogeneous blockchains to facilitate EHR sharing in a blockchain federation. Figure 12 shows the step-by-step process of the proposed method. Global smart contracts are unified contracts in the federation and are required to be deployed in each blockchain network. Global smart contracts are composed of different smart contracts across the networks that interoperate to share the data in a federation. The global smart contract in the proposed framework consists of three types of contracts, namely, conversion contract, connection contract, and transfer contract. In the proposed heterogeneous blockchain integration model, each platform runs a distinct business logic and architecture that accepts transactions in a predefined format. The conversion contract accepts the transaction in a local format that is used in the underlying platform and converts the local transaction to a uniform format that is compatible with the target blockchain network. The connection contract is designed to enable communication links between the source and target blockchains using the certificate authority (CA) address of the target blockchain. This module is triggered by the uniform transaction to perform the physical connection of networks and help the cross-chain communication protocol to transfer queries/data between the connected blockchains. The transfer contract is designed to store the transaction received from the target blockchain, which includes the EHR of the requested patient, encrypted using the public key of the CG from the source blockchain.

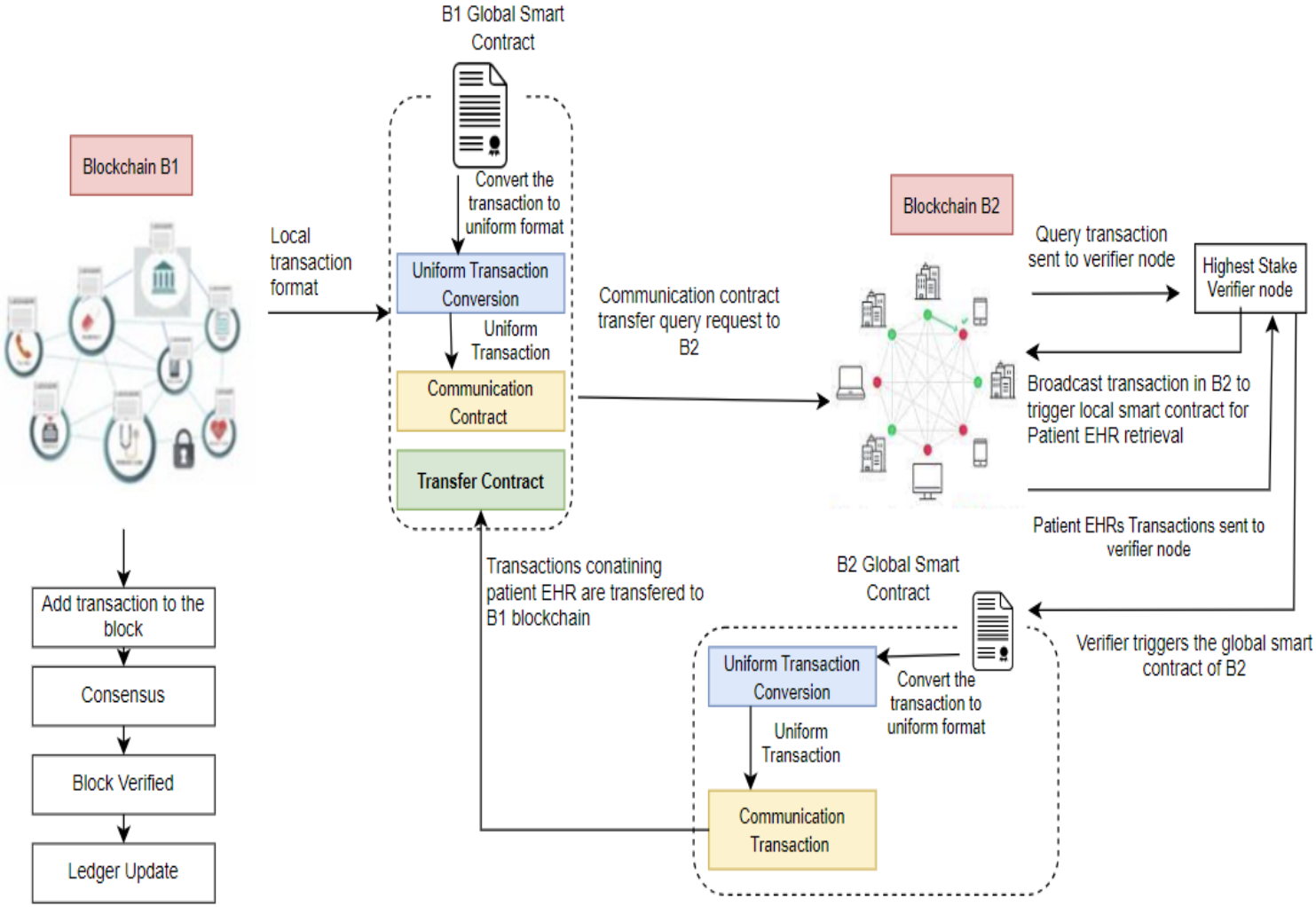


Figure 12: Proposed heterogeneous blockchains integration model for EHR sharing.

Once the transaction is broadcast in the target blockchain as a query from the source blockchain, the local smart contracts [ReadPatient()] of the target network are invoked, and the hash of the patient's EHR is added to the transaction; after transaction verification, the EHR is transferred to the transfer contract of the source blockchain via the cross-chain communication protocol. A cross-chain communication protocol does not make a direct state change of another blockchain network; instead, it triggers a set of functionalities on the other network that may result in the state change of the source blockchain. This set of functionalities is executed by triggering the SCs of the target blockchain, such as ReadPatientData() and AddPatientData(). In this paper, we focus on the sharing of EHR across heterogeneous blockchains; therefore, the cross-chain communication protocol triggers the ReadPatientData() function of the smart contract of the target blockchain. Modifying the EHRs in the external blockchain is not in the scope of this research.

2.6.1 Results and Discussion

The proposed interoperability model integrates heterogeneous blockchain platforms (HLF and Ethereum) to share EHRs in a federation. The performance of individual networks is evaluated based on the performance measures of TP, LT, and transaction success rate. The inter-blockchain communication is analyzed for ET at source blockchain.

The implementation of the proposed cross-chain interoperability is based on two independent blockchain networks using different platforms, Ethereum and HLF, to share the EHR of patients. Ethereum is used as a private test network to validate the proposed interoperability solution with the HLF consortium test network. The present work addresses interoperability challenges across different blockchain platforms to share patient EHR. To do so, HLF [100] and Ethereum [101] blockchain networks are integrated using an across-chain communication protocol. Both networks are deployed locally in a private/consortium mode for EHR sharing in the healthcare federation. The performance of each blockchain is evaluated using Hyperledger Caliper [102], an open-source benchmarking tool that measures the performance of blockchain networks. The software packages and dependencies used for implementing the proposed blockchain interoperability solution are Truffle Suit, Ganache, Solidity, Node 18.0.1, Hyperledger

Fabric V2.x, Git 2.9+, Python 2.7.x, Npm V 5.x, Docker Engine 17.037, Docker Compose 1.8+, VS code, and Hyperledger Caliper.

The individual performances of the two networks are evaluated and compared to show any impact on the inter-blockchain communication results. Hyperledger Caliper is used as a benchmark configuration; we set five worker nodes, run each experiment five times, then take the average. We conclude from the results that HLF is both a more highly scalable network and shows a higher TP than Ethereum.

The cross-chain communication ET is the time from when a transaction request is initiated in the source network (T_S) until a response is received from the target network (T_R), that is,

$ET = T_R - T_S$.

The interchain exchange requires the verification of transactions in a source chain from a target chain. Let T_{xn} be a transaction initiated at B1 to request a patient EHR residing at B2. Then, the elapsed time of cross-chain communication is calculated as a series of operations performed at B1 and B2, including the round-trip communication time (CT) from B1 to B2 and vice versa, that is:

$$ET = V_{B1}(T_{xn}) + CT_{(B1,B2)(B2,B1)} + V_{B2}(T_{xn}) + SC_{B2}(T_{xn}) + V_{B2}(RT_{xn}) + V_{B1}(RT_{xn}),$$

where $V_{B1}(T_{xn})$ is the time taken for the transaction validation at B1, and $V_{B2}(T_{xn})$ is the time taken for the transaction validation at B2; after validation, $SC_{B2}(T_{xn})$ is the time to trigger a smart contract at B2 to access the patient EHR for the query initiated from B1. RT_{xn} is the response transaction that includes the hash of the patient's record requested by B1, $V_{B2}(RT_{xn})$ is the response transaction validation at B2, and $V_{B1}(RT_{xn})$ is the response transaction validation at B1. $V_{B2}(T_{xn})$ and $V_{B1}(RT_{xn})$ are the transactions validated by external networks; therefore, the verifiers of the cross-chain communication protocol can make a request for the validator's public key and certificates of external networks for verification and to establish a trust relationship between the validators from both networks.

The query transaction is initiated from the HLF network to access the patient EHR from the Ethereum network. The first ET for query 1 is noted as higher than that of the other queries; this is for the first connection to the target network, and once the connection is

established the EL decreases, and the variation in ET is due to the query processing time (QT) at the target network. The calculated Ethereum QT is shown in Figure 13 paired against the ET.

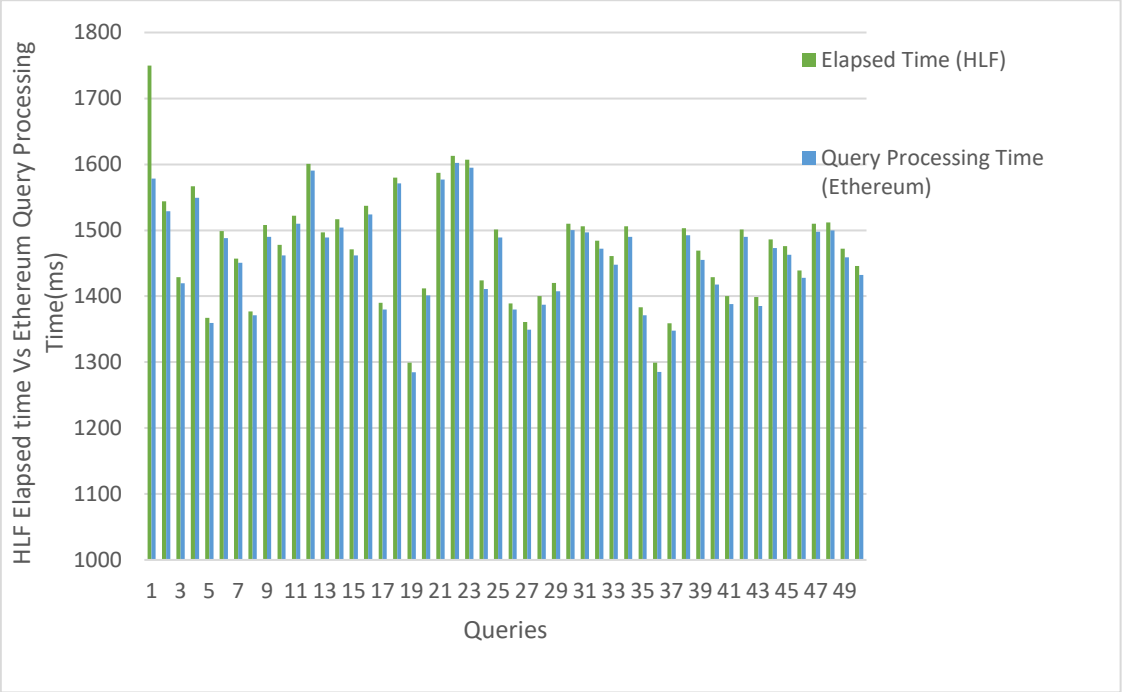


Figure 13: Inter-blockchain record access elapsed time vs. query processing time on the Ethereum network.

We compared the homogeneous and heterogenous blockchains' (based on the platforms) integration ET. The average ET for HLF to HLF is significantly lower than that for HLF to Ethereum because of the low performance of the Ethereum network, as demonstrated in Figure 14. This can be seen from the fact that the QT at the Ethereum network is higher than that of the HLF network. This results in a higher ET at the HLF network, the source network, communicating with the Ethereum network, which is the target network. The detailed results are provided in Article 3.

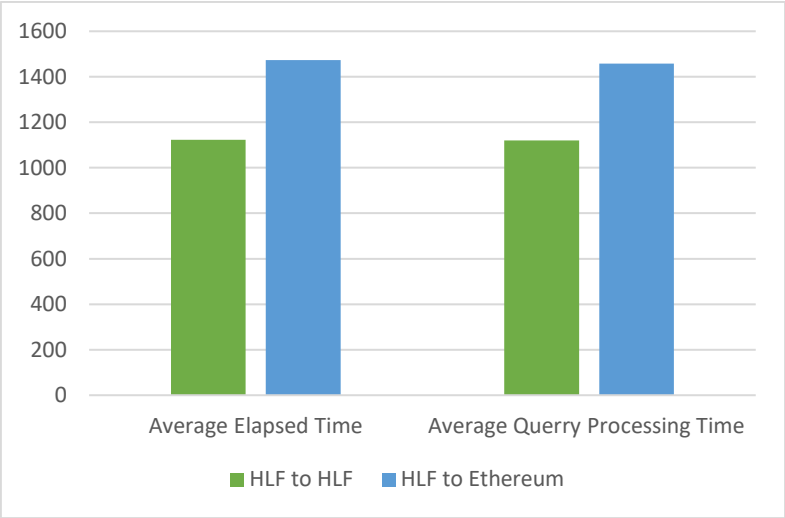


Figure 14: Comparison of ET and QT between Ethereum and HLF.

Redrafted from: Hashim, F., Shuaib, K., Baraka, E., and Sallabi, F., Integration of heterogeneous blockchains for sharing EHRs using transaction-based global smart contracts. (manuscript)

Chapter 3: Conclusion and Future Perspectives

The focus of this research is a healthcare blockchain federation comprised of multiple independent blockchain networks. Based on the research conducted in this study, we first addressed the scalability challenges in individual blockchain networks and then addressed the inter-blockchain communication in a federation of homogeneous and heterogeneous blockchain networks. Overall, we addressed these challenges at the transaction level. The proposed sharding-based solution processes the appointments in parallel, resulting in a significant increase in network TP and a decreased LT. The experimental results showed that our proposed sharded network processed 24 appointments per second whereas the unsharded network processed four appointments per second. This increase in appointment processing is due to the low LT of our proposed sharded solution, which is 83.33% lower than the unsharded network. Overall, a significant increase in TP of both sharded and unsharded networks is recorded, namely, 24TPS and 4TPS respectively. The proposed shard formation technique formed complete shards and successfully eliminated cross-shard communication in a sharded network.

PoA is a widely used consensus algorithm adopted in healthcare blockchains. The proposed instantaneous authority selection greatly improved the overall performance of the healthcare network as compared to traditional consensus algorithms, including PoW, PBFT, PoA(Aura), and PoA(Apla). We conducted experiments to perform a comparative analysis among the aforementioned algorithms. Our proposed improved PoA consensus algorithm recorded 0.3 sec consensus LT whereas PoA(Apla) and PoA(Aura) had 3.4 sec and 1.4 sec consensus LT, respectively. The TP performance of the proposed algorithm showed an increase of 56.4% over PoA(Aura) and 86.88% over PoA(Apla). Similarly, the average increase in the block generation of the proposed PoA algorithms is recorded as 108 blocks and 58 blocks over PoA(Apla) and PoA(Aura), respectively.

The proposed solutions to blockchain scalability have a significant impact on healthcare blockchain networks as they work at appointment level and increase the TP of the network, resulting in a high appointment processing rate. Sharding processes the appointments in parallel, and the instantaneous authority selection in the proposed PoA algorithm minimizes the consensus time and block generation time in healthcare. Healthcare is a

sensitive application domain as it deals with human life, and real-time solutions aid in the performance of healthcare blockchains.

Interoperability between independent blockchain networks is a challenging task as no layer 1 solution is available in the literature. In this study we proposed a blockchain federation to facilitate inter-blockchain communication to share EHR across diverse blockchain networks. We categorized the solution into homogeneous and heterogeneous network integration based on the platforms used to deploy the healthcare blockchain networks. A homogeneous blockchain integration is proposed using a transaction-based global smart contract triggering solution to share the EHR of a patient from independent HLF-to-HLF networks.

This study conducted an individual network performance followed by the inter-blockchain communication performance from one HLF network to another, such that both the networks are deployed via a different number of healthcare entities. Firstly, the results showed a minor increase in TP and a minor decrease in the consensus LT of the network with fewer healthcare entities. Due to the limited computational power of the CPU, the healthcare entities could not be increased to depict the significant change in TP and LT between both networks. As mentioned, this study addresses the interoperability at transaction level, such that the communication request is sent while an appointment is in progress. The query truncation was initiated from source network to target network, and the experimental results calculated the ET at source network. It is noted that the ET of first query transaction is 15.9% higher than that of the query transactions conducted thereafter. This increase is due to the initial connection to the target network. The heterogeneous blockchain network interoperability is performed using the HLF and Ethereum networks and global smart contracts. In the proposed solution a uniform conversion module is used to convert the local transaction format into a uniform transaction format to make it compatible with the target network. The initial connection to the Ethereum network is 18% higher than that of the other query transactions sent from HLF to Ethereum, which is 3% higher than the HLF-to-HLF first connection. The average ET of HLF to Ethereum is 26% higher than the HLF to HLF. This increase is due to the performance of the Ethereum network, which has a 15.6% TP decrease compared to the HLF network TP. Hence, the experimental results concluded that the ET depends on the QT of the target blockchain,

and the ET has a significance for homogeneous and heterogeneous network interoperability.

Finally, we compare the LT of our proposed homogeneous and heterogeneous solutions to previous work [56], and the experimental results showed the LT improved over that shown in that study by 78.09% and 52.63% for homogeneous and heterogeneous integration, respectively.

The key contributions of this dissertation can be stated as follows. The author introduced the sharding technique into a healthcare blockchain network to process appointments in parallel and proposed an authority selection process in a PoA consensus algorithm to address the scalability challenges in healthcare blockchains as the number of nodes increases in the network. Both techniques resulted in high TP and provided a healthcare-specific solution for scalable healthcare networks. The scalability solutions are provided for an individual network in federation. Secondly, the author introduced an interoperability solution to integrate health blockchains in a federation of homogeneous and heterogeneous networks. Inter-blockchain communication is performed between blockchains deployed via same and different platforms using a unified integration mechanism at the transaction level.

3.1 Limitations

The limitations of this study are summarized as follows:

- The experimental results of the proposed healthcare blockchain sharding approach and improved PoA consensus algorithm are limited to the Python simulation. These solutions could not be implemented using blockchain platforms due to the limited CPU power of the systems used for experimentation. The scalability test required an increasing number of nodes in the network; however, increasing a single healthcare entity using the blockchain platforms consumed maximum CPU power and resulted in failed transactions. Therefore, a minimal blockchain network was simulated using Python to test the performance of the proposed scalability solutions in healthcare.
- The current study uses two types of blockchain platforms for heterogeneous blockchains integration in healthcare federation (HLF and Ethereum). Due to the

complexity of blockchain platforms and time constraints on this research, other platforms could not be investigated for integration.

- This study utilized simulated EHRs (text records) to develop robust interoperability solutions. Although the current implementation involved simulated data, the future plans involve expanding the solution to incorporate actual EHR data sets, encompassing both text and images, within a healthcare federation.
- Blockchain addresses are identified by public keys. The patient public key is used to request EHR in the network. However, this study uses patient ID (national identity card number/citizenship number) to request EHR from an external blockchain. Each blockchain network generates a unique public/private key pair in a network that is not known in any external network. Therefore, we used patient ID, which is uniform across a country/state. Once the transaction is transferred to the target network, the patient ID is replaced with the patient public key generated by the underlying network.

While these limitations should be acknowledged, they provide opportunities for further research and potential improvements in future studies. Addressing these limitations would enhance the applicability and real-world evaluation of the proposed solutions in healthcare blockchain networks.

3.2 Future Research

The following recommendations are suggested for future studies:

3.2.1 Expansion of Inter-Blockchain Communication Solutions

Extend the current inter-blockchain communication solutions by incorporating additional blockchain platforms such as Hyperledger Sawtooth, IBM Blockchain, R3 Corda, and Stellar. Investigate the compatibility and effectiveness of edge computing and IoT devices in the context of healthcare blockchain federations, aiming to enhance interoperability and expand the range of integration possibilities. Further research investigation is needed in developing incentive mechanisms, enabling interoperability with legacy systems, improving disaster recovery and fault tolerance, and promoting standardization and best practices across industry.

3.2.2 Exploration of EHR Management Solutions in Blockchain Federations

Focus on exploring EHR management solutions within the context of blockchain federations. Address the challenges associated with the data format for EHR in a federation of independent and heterogeneous blockchain networks. Consider extending the uniform integration approach to enable efficient EHR management and sharing within the federation, taking into account data consistency, privacy, and security.

3.2.3 Utilization of Actual EHR Datasets

Implement and improve the current interoperability solution using actual EHR datasets for each node in the network. By employing real-world EHR data, researchers can evaluate the performance, scalability, and effectiveness of the proposed solutions in a more realistic setting. This would provide valuable insights into the practical applicability of the solutions and their impact on healthcare data management.

3.2.4 Integration of AI Techniques

Explore the integration of artificial intelligence (AI) techniques within the blockchain federation. Utilize AI to enhance the functionality and efficiency of the network, such as locating the target networks previously visited by the patient or accelerating the process of searching for EHRs within the dataset. Investigate the potential benefits of AI integration in terms of speed, accuracy, and resource optimization.

3.2.5 Development of Unified Public/Private Key Solutions

Investigate solutions to generate a unified public/private key pair in a federation. Aim to establish a mechanism where all the blockchains within the federation operate with a single set of public/private keys associated with the patient. This unified approach would significantly facilitate interoperability beyond geographical boundaries, enabling seamless data sharing and access across disparate healthcare blockchain networks.

By pursuing these recommendations, future research endeavors can advance the field of healthcare blockchain, address existing challenges, and pave the way for more efficient, secure, and interconnected healthcare systems.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Accessed: Jul. 06, 2022. [Online]. Available: www.bitcoin.org

[2] O. Dib, A. Durand, K.-L. Brousmiche, E. Thea, and B. Hamida,“Consortium Blockchains: Overview, applications and challenges. *Int. J. Adv. Telecommun*, *11*(1), pp.51-64, 2018, Accessed: Mar. 06, 2023. [Online]. Available: http://www.iariajournals.org/telecommunications/2018

[3] K. Shuaib, H. Saleous, K. Shuaib, and N. Zaki, “Blockchains for Secure Digitized Medicine,” *J. Pers. Med. 2019,* vol. 9, no. 3, pp. 35, Jul. 2019, doi: 10.3390/JPM9030035.

[4] L. Ismail, H. Materwala, and S. Zeadally, “Lightweight Blockchain for Healthcare,” *IEEE Access*, vol. 7, pp. 149935–149951, 2019, doi: 10.1109/ACCESS.2019.2947613.

[5] J. D. Dubin, “Blockchain Prediction Markets: Where They Came from, Why They Matter & How to Regulate Those Involved,” *Washingt. Univ. Law Rev.*, vol. 97, 2019, Accessed: Mar. 16, 2023. [Online]. Available: https://heinonline.org/HOL/Page?handle=hein.journals/walq97&id=589&div=&collection=

[6] A. Carvalho, “A Permissioned Blockchain-Based Implementation Of LMSR Prediction Markets,” *Decis. Support Syst.*, vol. 130, pp. 113228, Mar. 2020, doi: 10.1016/J.DSS.2019.113228.

[7] V. Chakravaram, S. Ratnakaram, E. Agasha, and N. S. Vihari, “The Role of Blockchain Technology in Financial Engineering,” *Lect. Notes Electr. Eng.*, vol. 698, pp. 755–765, 2021, doi: 10.1007/978-981-15-7961-5_72/COVER.

[8] B. Notheisen, F. Hawlitschek, and C. Weinhardt, “Association for Information Systems AIS Electronic Library (AISeL) Breaking Down The Blockchain Hype-Towards A Blockchain Market Engineering Approach,” 2017, Accessed: Mar. 16, 2023. [Online]. Available: http://aisel.aisnet.org/ecis2017_rp/69

[9] M. E. Salcedo *et al.*, “Blockchain and Information Systems”. Americas Conference on Information Systems, 2018. Accessed: Jan. 16, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Blockchain-and-Information-Systems-Salcedo-Pineda/782ea4844bf01697decdb5acbde636a9d3c6e0e1

[10] H. Subramanian, “Decentralized Blockchain-Based Electronic Marketplaces Decentralized Blockchain-Based Electronic Marketplac-es from CACM,” *Commun. ACM*, vol. 61, no. 1, pp. 78–84, doi: 10.1145/3158333.

[11] S. Tanwar, K. Parekh, and R. Evans, “Blockchain-Based Electronic Healthcare Record System For Healthcare 4.0 Applications,” *J. Inf. Secur. Appl.*, vol. 50, pp. 102407, Feb. 2020, doi: 10.1016/J.JISA.2019.102407.

[12] M. Andoni *et al.*, “Blockchain Technology In The Energy Sector: A Systematic Review Of Challenges And Opportunities,” *Renew. Sustain. Energy Rev.*, vol. 100, pp. 143–174, Feb. 2019, doi: 10.1016/J.RSER.2018.10.014.

[13] Q. Wang and M. Su, “Integrating Blockchain Technology Into The Energy Sector — From Theory Of Blockchain To Research And Application Of Energy Blockchain,” *Comput. Sci. Rev.*, vol. 37, pp. 100275, Aug. 2020, doi: 10.1016/J.COSREV.2020.100275.

[14] M. M. Queiroz, R. Telles, and S. H. Bonilla, “Blockchain And Supply Chain Management Integration: A Systematic Review Of The Literature,” *Supply Chain Manag.*, vol. 25, no. 2, pp. 241–254, Feb. 2020, doi: 10.1108/SCM-03-2018-0143/FULL/PDF.

[15] P. Dutta, T. M. Choi, S. Somani, and R. Butala, “Blockchain Technology In Supply Chain Operations: Applications, Challenges And Research Opportunities,” *Transp. Res. Part E Logist. Transp. Rev.*, vol. 142, pp. 102067, Oct. 2020, doi: 10.1016/J.TRE.2020.102067.

[16] H. Xiong, T. Dalhaus, P. Wang, and J. Huang, “Blockchain Technology for Agriculture: Applications and Rationale,” *Front. Blockchain*, vol. 3, pp. 7, Feb. 2020, doi: 10.3389/FBLOC.2020.00007.

[17] F. Antonucci, S. Figorilli, C. Costa, F. Pallottino, L. Raso, and P. Menesatti, “A Review On Blockchain Applications In The Agri-Food Sector,” *J. Sci. Food Agric.*, vol. 99, no. 14, pp. 6129–6138, Nov. 2019, doi: 10.1002/JSFA.9912.

[18] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using Blockchain For Medical Data Access And Permission Management,” *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, Sep. 2016, doi: 10.1109/OBD.2016.11.

[19] “Medicalchain Whitepaper 2.1,” 2018. Accessed: Mar. 18, 2022. [Online]. Available: https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf

[20] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control,” *J. Med. Syst.*, vol. 40, no. 10, pp. 1–8, Oct. 2016, doi: 10.1007/S10916-016-0574-6/METRICS.

[21] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, “MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain,” *J. Med. Syst. 2018 428*, vol. 42, no. 8, pp. 1–11, Jun. 2018, doi: 10.1007/S10916-018-0993-7.

[22] B. Shen, J. Guo, and Y. Yang, “MedChain: Efficient Healthcare Data Sharing via Blockchain,” *Appl. Sci. 2019, Vol. 9, Page 1207*, vol. 9, no. 6, pp. 1207, Mar. 2019, doi: 10.3390/APP9061207.

[23] M. Zamani, M. Movahedi, and M. Raykova, “RapidChain: Scaling Blockchain Via Full Sharding,” *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 931–948, Oct. 2018, doi: 10.1145/3243734.3243853.

[24] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, “A Secure Sharding Protocol For Open Blockchains,” *Proc. ACM Conf. Comput. Commun. Secur.*, vol. 24-28-October-2016, pp. 17–30, Oct. 2016, doi: 10.1145/2976749.2978389.

[25] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, “OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding,” *Proc. - IEEE Symp. Secur. Priv.*, vol. 2018-May, pp. 583–598, Jul. 2018, doi: 10.1109/SP.2018.000-5.

[26] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, and G. Danezis, “Chainspace: A Sharded Smart Contract Platform”. In *Network and Distributed System Security Symposium* 2018 (NDSS 2018) 2018.

[27] J. Wang and H. Wang, "Monoxide: Scale Out Blockchains With Asynchronous Consensus Zones." In *16th USENIX symposium on networked systems design and implementation (NSDI 19)*, pp. 95-112. 2019. Accessed: Mar. 15, 2023. [Online]. Available: https://www.usenix.org/conference/nsdi19/presentation/wang-jiaping

[28] W. Tong, X. Dong, Y. Shen, and X. Jiang, “A Hierarchical Sharding Protocol for Multi-Domain IoT Blockchains,” *IEEE Int. Conf. Commun.*, vol. 2019-May, May 2019, doi: 10.1109/ICC.2019.8761147.

[29] F. Hashim, K. Shuaib, and N. Zaki, “Sharding for Scalable Blockchain Networks,” *SN Comput. Sci.*, vol. 4, no. 1, pp. 1–17, Jan. 2023, doi: 10.1007/S42979-022-01435-Z/METRICS.

[30] S. Li, M. Yu, C. S. Yang, A. S. Avestimehr, S. Kannan, and P. Viswanath, “PolyShard: Coded Sharding Achieves Linearly Scaling Efficiency and Security Simultaneously,” *IEEE Trans. Inf. Forensics Secur.*, vol. 16, pp. 249–261, 2021, doi: 10.1109/TIFS.2020.3009610.

[31] M. J. Amiri, D. Agrawal, and A. El Abbadi, “SharPer: Sharding Permissioned Blockchains over Network Clusters,” *Proc. ACM SIGMOD Int. Conf. Manag. Data*, pp. 76–88, 2021, doi: 10.1145/3448016.3452807.

[32] X. Cai *et al.*, “A Sharding Scheme-Based Many-Objective Optimization Algorithm for Enhancing Security in Blockchain-Enabled Industrial Internet of Things,” *IEEE Trans. Ind. Informatics*, vol. 17, no. 11, pp. 7650–7658, Nov. 2021, doi: 10.1109/TII.2021.3051607.

[33] A. Manuskin, M. Mirkin, and I. Eyal, “Ostraka: Secure Blockchain Scaling by Node Sharding,” *Proc. - 5th IEEE Eur. Symp. Secur. Priv. Work. Euro S PW 2020*, pp. 397–406, Sep. 2020, doi: 10.1109/EUROSPW51379.2020.00060.

[34] B. Ghimire, D. B. Rawat, C. Liu, and J. Li, “Sharding-Enabled Blockchain for Software-Defined Internet of Unmanned Vehicles in the Battlefield,” *IEEE Netw.*, vol. 35, no. 1, pp. 101–107, Mar. 2021, doi: 10.1109/MNET.011.2000214.

[35] F. Hashim, K. Shuaib, and F. Sallabi, “MedShard: Electronic Health Record Sharing Using Blockchain Sharding,” *Sustain. 2021,* pp. 5889, vol. 13, no. 11, May 2021, doi: 10.3390/SU13115889.

[36] M. N. Halgamuge, S. C. Hettikankanamge, and A. Mohammad, “Trust Model to Minimize the Influence of Malicious Attacks in Sharding Based Blockchain Networks,” *Proc. - 2020 IEEE 3rd Int. Conf. Artif. Intell. Knowl. Eng. AIKE 2020*, pp. 162–167, Dec. 2020, doi: 10.1109/AIKE48582.2020.00032.

[37] J. Zhang, Z. Hong, X. Qiu, Y. Zhan, S. Guo, and W. Chen, “SkyChain: A Deep Reinforcement Learning-Empowered Dynamic Blockchain Sharding System,” *ACM Int. Conf. Proceeding Ser.*, vol. 20, Aug. 2020, doi: 10.1145/3404397.3404460.

[38] S. Kantesariya and D. Goswami, “Determining Optimal Shard Size in a Hierarchical Blockchain Architecture,” *IEEE Int. Conf. Blockchain Cryptocurrency, ICBC 2020*, May 2020, doi: 10.1109/ICBC48266.2020.9169448.

[39] G. W.-E. project yellow paper and undefined 2014, “Ethereum: A secure decentralised generalised transaction ledger,” *files.gitter.im*. Accessed: Mar. 15, 2023. [Online]. Available: https://files.gitter.im/ethereum/yellowpaper/VIyt/Paper.pdf

[40] M. Milojkovic, “Privacy-Preserving Framework for Access Control and Interoperability of Electronic Health Records Using Blockchain Technology,” *Showc. Undergrad. Res. Creat. Endeavors*, Apr. 2018. Accessed: Mar. 15, 2023. [Online]. Available: https://digitalcommons.winthrop.edu/source/SOURCE_2018/posterpresentations/64

[41] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, “Blockchain-Based Data Preservation System for Medical Data,” *J. Med. Syst.*, vol. 42, no. 8, pp. 1–13, Aug. 2018, doi: 10.1007/S10916-018-0997-3/METRICS.

[42] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, “HealthSense: A medical use case of Internet of Things and blockchain,” *Proc. Int. Conf. Intell. Sustain. Syst. ICISS 2017*, pp. 486–491, Jun. 2018, doi: 10.1109/ISS1.2017.8389459.

[43] Y. Ji, J. Zhang, J. Ma, C. Yang, and X. Yao, “BMPLS: Blockchain-Based Multi-level Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems,” *J. Med. Syst.*, vol. 42, no. 8, pp. 1–13, Aug. 2018, doi: 10.1007/S10916-018-0998-2/METRICS.

[44] S. King and S. Nadal, “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,” 2012. Accessed: Jan. 23, 2023. [Online]. Available: https://peercoin. net/assets/paper/peercoin-paper. pdf.

[45] V. Patel and R. Reagan, “A Framework For Secure And Decentralized Sharing Of Medical Imaging Data Via Blockchain Consensus,” *Health Informatics J.*, vol. 25, no. 4, pp. 1398–1411, 2019, doi: 10.1177/1460458218769699.

[46] M. Zghaibeh, U. Farooq, N. U. Hasan, and I. Baig, “SHealth: A Blockchain-Based Health System with Smart Contracts Capabilities,” *IEEE Access*, vol. 8, pp. 70030–70043, 2020, doi: 10.1109/ACCESS.2020.2986789.

[47] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain.” In *CEUR workshop proceedings*, vol. 2058. CEUR-WS, 2018.

[48] N. Al Asad, M. T. Elahi, A. Al Hasan, and M. A. Yousuf, “Permission-Based Blockchain With Proof Of Authority For Secured Healthcare Data Sharing,” *2020 2nd Int. Conf. Adv. Inf. Commun. Technol. ICAICT 2020*, pp. 35–40, Nov. 2020, doi: 10.1109/ICAICT51780.2020.9333488.

[49] J. N. Al-Karaki, A. Gawanmeh, M. Ayache, and A. Mashaleh, “DASS-CARE: A Decentralized, Accessible, Scalable, And Secure Healthcare Framework Using Blockchain,” *2019 15th Int. Wirel. Commun. Mob. Comput. Conf. IWCMC 2019*, pp. 330–335, 2019, doi: 10.1109/IWCMC.2019.8766714.

[50] M. Borkowski, M. Sigwart, P. Frauenthaler, T. Hukkinen, and S. Schulte, “Dextt: Deterministic Cross-Blockchain Token Transfers,” *IEEE Access*, vol. 7, pp. 111030–111042, 2019, doi: 10.1109/ACCESS.2019.2934707.

[51] S. Yang, H. Wang, W. Li, W. Liu, … X. F. C. C. and I. of, and undefined 2018, “CVEM: A Cross-Chain Value Exchange Mechanism,” *dl.acm.org*, pp. 80–85, Oct. 2018, doi: 10.1145/3291064.3291073.

[52] “Welcome to ICON! | ICON Community.” Accessed: Jan. 25, 2023. [Online]. Available: https://icon.community/

[53] “Crypto Solutions for Business | Ripple.” Accessed: Sept. 15, 2021. [Online]. Available:https://ripple.com/

[54] “Metronome: The Built-to-Last Cryptocurrency.” Accessed: Dec. 5, 2022. [Online]. Available: https://www.metronome.io/

[55] D. Ding, T. Duan, L. Jia, K. Li, Z. Li, and Y. Sun, “InterChain: A Framework to Support Blockchain Interoperability”. *Second Asia-Pacific Work. Netw*, 2018. Accessed: Jun. 15, 2022. [Online]. Available: https://icowhitepapers.co/wp-content/uploads/

[56] “Cosmos: The Internet of Blockchains.” Accessed: Dec. 5, 2022. [Online]. Available: https://cosmos.network/

[57] A. . Fallis, “Rootstock Platform: Bitcoin Powered Smart Contracts - White Paper,” *J. Chem. Inf. Model.*, vol. 53, no. 9, pp. 1689–1699, 2015.

[58] “Bitcoin’s leading sidechain, enabling fast, confidential transactions, and the issuance of assets.” Accessed: Jan. 4, 2023. [Online]. Available: https://blockstream.com/liquid/

[59] “Elements | elementsproject.org.” Accessed: Dec. 5, 2022. [Online]. Available: https://elementsproject.org/

[60] A. Back *et al.*, “Enabling Blockchain Innovations with Pegged Sidechains,” 2014. Accessed: August. 20, 2022. [Online]. Available: http://kevinriggen.com/files/sidechains.pdf

[61] “Loom Network – Production-Ready, Multichain Interop Platform for Serious Dapp Developers.” Accessed: Dec. 5, 2022. [Online]. Available: https://loomx.io/

[62] “POA Merger & Swap Notice - POA.” Accessed: Dec. 5, 2022. [Online]. Available: https://www.poa.network/

[63] M. A. Talib *et al.*, “Interoperability Among Heterogeneous Blockchains: A Systematic Literature Review,” *EAI/Springer Innov. Commun. Comput.*, pp. 135–166, 2021, doi: 10.1007/978-3-030-75107-4_6/COVER.

[64] G. G. Dagher, C. L. Adhikari, and T. Enderson, “Towards Secure Interoperability between Heterogeneous Blockchains using Smart Contracts,” In *Future Technologies Conference (FTC)*, vol. 2017, pp. 73-81. 2017.

[65] W. Li, A. Sforzin, S. Fedorov, and G. O. Karame, “Towards Scalable and Private Industrial Blockchains,” *Proc. ACM Work. Blockchain, Cryptocurrencies Contract.*, doi: 10.1145/3055518.

[66] “An Analysis of Atomic Swaps on and between Ethereum Blockchains using Smart Contracts,” 2018, vol 11, pp. 2017-2018, Technical report 2018. Accessed: Oct. 10, 2022. [Online]. Available: https://rp.os3.nl/2017-2018/p42/report.pdf

[67] P. Robinson, R. Ramesh, and S. Johnson, “Atomic Crosschain Transactions for Ethereum Private Sidechains,” *Blockchain Res. Appl.*, vol. 3, no. 1, pp. 100030, Mar. 2022, doi: 10.1016/J.BCRA.2021.100030.

[68] M. Herlihy, “Atomic cross-chain swaps,” *Proc. Annu. ACM Symp. Princ. Distrib. Comput.*, pp. 245–254, Jul. 2018, doi: 10.1145/3212734.3212736.

[69] “Home - Blocknet Documentation.”, Accessed: Dec. 5, 2022. [Online]. Available: https://docs.blocknet.org/

[70] “Introduction - Wanchain.”, Accessed: Dec. 5, 2022. [Online]. Available: https://docs.wanchain.org/get-started/introduction

[71] “ 1 - What is AION Blockchain? The Most Comprehensive Guide Ever -.”, Accessed: Dec. 5, 2022. [Online]. Available: https://www.blockchain-council.org/blockchain/aion-blockchain/

[72] “ARK.io | A Blockchain Ecosystem Built For Everyone.”, Accessed: Dec. 5, 2022. [Online]. Available: https://ark.io/

[73] H. Wang, Y. Cen, and X. Li, “Blockchain router: A cross-chain communication protocol,” *ACM Int. Conf. Proceeding Ser.*, vol. Part F128273, pp. 94–97, Mar. 2017, doi: 10.1145/3070617.3070634.

[74] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao, and H. Kai, “A Multiple Blockchains Architecture on Inter-Blockchain Communication,” *Proc. - 2018 IEEE 18th Int. Conf. Softw. Qual. Reliab. Secur. Companion, QRS-C 2018*, pp. 139–145, Aug. 2018, doi: 10.1109/QRS-C.2018.00037.

[75] “Anlink Blockchain Network Whitepaper V 1.0,” 2017. Accessed: Sep. 1, 2022. [Online]. Available: https://alicliimg.clewm.net/049/389/1389049/1484820492640c2baf37ea3e4f9fd77bd52c2a1e9bbbe1484820484.pdf

[76] M. Madine, K. Salah, R. Jayaraman, Y. Al-Hammadi, J. Arshad, and I. Yaqoob, “AppxChain: Application-level interoperability for blockchain networks,” *IEEE Access*, vol. 9, pp. 87777–87791, 2021, doi: 10.1109/ACCESS.2021.3089603.

[77] J. Poon and V. Buterin, “Plasma: Scalable Autonomous Smart Contracts,” White Paper, 2017.Accessed: Jun. 15, 2022. [Online]. Available: https://plasma.io/

[78] L. Deng, H. Chen, J. Zeng, and L. J. Zhang, “Research on cross-chain technology based on sidechain and hash-locking,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10973 LNCS, pp. 144–151, 2018, doi: 10.1007/978-3-319-94340-4_12/COVER/.

[79] Z. CHEN, Z. YU, Z. DUAN, and K. HU, “Inter-Blockchain Communication,” *DEStech Trans. Comput. Sci. Eng.*, no. cst, pp. 448–454, 2017, doi: 10.12783/dtcse/cst2017/12539.

[80] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, “Algorand: Scaling Byzantine Agreements for Cryptocurrencies,” *SOSP 2017 - Proc. 26th ACM Symp. Oper. Syst. Princ.*, pp. 51–68, Oct. 2017, doi: 10.1145/3132747.3132757.

[81] L. N. Nguyen, T. D. T. Nguyen, T. N. Dinh, and M. T. Thai, “OptChain: Optimal transactions placement for scalable blockchain sharding,” *Proc. - Int. Conf. Distrib. Comput. Syst.*, vol. 2019-July, pp. 525–535, Jul. 2019, doi: 10.1109/ICDCS.2019.00059.

[82] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, “Applications of Blockchains in the Internet of Things: A Comprehensive Survey,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1676–1717, Apr. 2019, doi: 10.1109/COMST.2018.2886932.

[83] J. Mattila, “The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures,” 2016, Accessed: Mar. 15, 2023. [Online]. Available: https://www.econstor.eu/handle/10419/201253

[84] X. Zhu, J. Shi, and C. Lu, “Cloud Health Resource Sharing Based on Consensus-Oriented Blockchain Technology: Case Study on a Breast Tumor Diagnosis Service,” *J Med Internet Res 2019;21(7)e13767,* vol. 21, no. 7, pp. e13767, Jul. 2019 *https//www.jmir.org/2019/7/e13767*, doi: 10.2196/13767.

[85] “SHA-256 Cryptographic Hash Algorithm implemented in JavaScript | Movable Type Scripts.”, Accessed: Mar. 15, 2023. [Online]. Available: https://www.movable-type.co.uk/scripts/sha256.html

[86] “Aura - Authority Round · OpenEthereum Documentation.”, Accessed: Mar. 15, 2023. [Online]. Available: https://openethereum.github.io/Aura

[87] “Proof-of-Authority consensus — Apla Blockchain Platform Guide documentation.”, Accessed: Jan. 12, 2023. [Online]. Available: https://apla.readthedocs.io/en/latest/concepts/consensus.html

[88] T. Fatokun, A. Nag, and S. Sharma, “Towards a Blockchain Assisted Patient Owned System for Electronic Health Records,” *Electron. 2021,* vol. 10, no. 5, pp. 580, Mar. 2021, doi: 10.3390/ELECTRONICS10050580.

[89] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, “Blockchain-Based Data Preservation System for Medical Data,” *J. Med. Syst. 2018 428*, vol. 42, no. 8, pp. 1–13, Jun. 2018, doi: 10.1007/S10916-018-0997-3.

[90] S. Rouhani, “MediChain TM : A Secure Decentralized Medical Data Asset Management System,” *2018 IEEE Int. Conf. Internet Things IEEE Green Comput. Commun. IEEE Cyber, Phys. Soc. Comput. IEEE Smart Data*, no. Section II, pp. 1533–1538, 2018, doi: 10.1109/Cybermatics.

[91] K. Shuaib, J. Abdella, F. Sallabi, and M. A. Serhani, “Secure decentralized electronic health records sharing system based on blockchains,” *J. King Saud Univ. - Comput. Inf. Sci.*, May 2021, doi: 10.1016/J.JKSUCI.2021.05.002.

[92] “A Blockchain Platform for the Enterprise — hyperledger-fabricdocs main documentation.”, Accessed: Jan. 12, 2023. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/

[93] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. Habib ur Rehman, and C. A. Kerrache, “The Case Of Hyperledger Fabric As A Blockchain Solution For Healthcare Applications,” *Blockchain Res. Appl.*, vol. 2, no. 1, pp. 100012, Mar. 2021, doi: 10.1016/J.BCRA.2021.100012.

[94] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, “Hyperledger Fabric Blockchain for Securing the Edge Internet of Things,” *Sensors 2021,* vol. 21, no. 2, pp. 359, Jan. 2021, doi: 10.3390/S21020359.

[95] S. Figueroa-Lorenzo, J. A. Benito, and S. Arrizabalaga, “Modbus Access Control System Based on SSI over Hyperledger Fabric Blockchain,” *Sensors 2021, Vol. 21, Page 5438*, vol. 21, no. 16, pp. 5438, Aug. 2021, doi: 10.3390/S21165438.

[96] A. S. Podda and L. Pompianu, “An Overview Of Blockchain-Based Systems And Smart Contracts For Digital Coupons,” *Proc. - 2020 IEEE/ACM 42nd Int. Conf. Softw. Eng. Work. ICSEW 2020*, vol. 20, pp. 770–778, Jun. 2020, doi: 10.1145/3387940.3391500.

[97] D. Ravi, S. Ramachandran, R. Vignesh, V. R. Falmari, and M. Brindha, “Privacy Preserving Transparent Supply Chain Management Through Hyperledger Fabric,” *Blockchain Res. Appl.*, vol. 3, no. 2, pp. 100072, Jun. 2022, doi: 10.1016/J.BCRA.2022.100072.

[98] S. Schulte, M. Sigwart, P. Frauenthaler, M. Borkowski, "Towards blockchain interoperability". In Business Process Management: Blockchain and Central and Eastern Europe Forum: BPM 2019 Blockchain and CEE Forum, Vienna, Austria, September 1–6, 2019, Proceedings 17 2019, pp. 3-10. Springer International Publishing. M. B. E. E. F. B. 2019 B.

[99] F. Hashim, K. Shuaib, and F. Sallabi, “Connected Blockchain Federations for Sharing Electronic Health Records,” *Cryptogr. 2022,* vol. 6, no. 3, pp. 47, Sep. 2022, doi: 10.3390/CRYPTOGRAPHY6030047.

[100] “A Blockchain Platform for the Enterprise — hyperledger-fabricdocs main documentation." Accessed: Jan. 12, 2023. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.5/

[101] “Home | ethereum.org.” Accessed: Jan. 12, 2023. [Online]. Available: https://ethereum.org/en/

[102] “Hyperledger Caliper – Hyperledger Foundation.” Accessed: Jan. 12, 2023. [Online]. Available: https://www.hyperledger.org/use/caliper

List of Other Publications

Hashim, F., Shuaib, K., and Zaki, N., "Sharding for Scalable Blockchain Networks," *SN Comput. Sci.*, vol. 4, no. 1, pp. 1–17, Jan. 2023, doi: 10.1007/S42979-022-01435-Z/METRICS.

UAE UNIVERSITY DOCTORATE DISSERTATION NO. 2023:35

Efficient sharing of Electronic Health Records (EHRs) is vital in the healthcare industry. In this regard, blockchain-enabled healthcare federation uses a transaction-based global smart-contract triggering solution for seamlessly exchanging EHRs among patients and caregivers across local and external blockchain networks.

Faiza Hashim received her Ph.D. degree in Informatics and Computing from the Department of Computer Science and Software Engineering, College of Information Technology at UAE University, UAE. She received her master's degree in Information Technology from the Department of Computer Science, Peshawar University, Pakistan.