International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. , No. (Mon-20..)

http://dx.doi.org/10.12785/ijcds/XXXXXX

Enhancing EHR Sharing through Interconnected Blockchains via Global Smart Contracts

Faiza Hashim[1], **Khaled Shuaib**[1], **Ezedin Baraka**[1] **and Farag Sallabi**[1]

[1]*College of Information Technology,United Arab Emirates University, Al Ain, UAE*

Received Mon. 20, Revised Mon. 20, Accepted Mon. 20, Published Mon. 20

Abstract: Blockchain technology has ushered in transformative possibilities within the healthcare sector by creating a unified distributed network that streamlines the exchange of patient data among various stakeholders. However, the adoption of private or consortium-based blockchain models has raised concerns about the potential isolation and fragmentation of these networks. To address this challenge, blockchain interoperability has emerged as an escalating research area that offers a means for independent blockchains to collaborate across diverse platforms within a federated ecosystem. This study proposed a novel cross-chain communication (CCC) protocol designed to integrate independent blockchains operating on different platforms. By leveraging a global smart-contract triggering mechanism, this protocol establishes a standardized transaction conversion module to ensure transaction compatibility across various blockchain platforms within a federated network. The practical implementation of our CCC protocol was demonstrated through the exchange of electronic health records between the Hyperledger Fabric and Ethereum networks. Extensive experimentation was conducted to assess the performance metrics, revealing critical dependencies between the source and target blockchain networks in terms of the average elapsed time and query processing duration within the target network. The findings of this study underscore the considerable potential of blockchain interoperability within a federation, particularly when applied to the sharing of patient EHRs dispersed across multiple autonomous blockchains.

Keywords: Blockchains integration, cross-chain communication, electronic health record sharing, inter-blockchain communication, global smart contract.

1. INTRODUCTION

Blockchains are digital ledger systems that provide secure, decentralized, and tamper-proof records without the need for a central authority [1]. They have garnered significant interest from both industry and academia, particularly in ensuring data integrity between entities. The adaptability of blockchain technology has allowed it to be applied in a variety of domains, including healthcare, where it has been used to address privacy and security concerns. Despite the rapid growth of blockchain technology in healthcare [2] [3] [4] [5] [6] [7] [8] [9] [10], the vast majority of healthcare blockchains currently exist as separate, non-interoperable systems, resulting in suboptimal sharing and utilization of digital assets across various networks. To address this issue, the development of interoperable blockchain networks is essential to enable seamless sharing and use of digital assets/data across different independent blockchain networks. The integration of blockchain technology with other technologies such as the Internet of Things (IoT) and artificial intelligence (AI) can further enhance the potential of blockchain technology in healthcare and other domains. As the use of blockchain technology continues to evolve, it is important to address the challenges associated with its implementation to realize its potential benefits fully.

An inter-blockchain communication (IBC) technique is being used as a solution to these problems, and the integration of a diverse group of blockchains is known as inter-blockchain communication [11] [12] [13] [14]. Interoperability in blockchain technology has the potential to bring about a significant shift in open systems, allowing for seamless communication and interaction between devices and users across blockchain platforms. Although present IBC solutions are limited to working with the same platforms and do not support interoperability between diverse platforms, this restriction creates difficulties in conducting transactions across a variety of blockchain networks in a federation. This can have significant consequences, for instance, a patient's medical record that is stored on one blockchain may not be immediately accessible from another blockchain that operates on a different platform when needed. At present, there are no layer-1 blockchain solutions that can facilitate transactions on another blockchain and

invoke smart-contracts across different blockchains [15].
Blockchain has many appealing properties that could be used to achieve better interoperability with enhanced capacity, data sharing, access, and control among the referenced partners. Interoperability is crucial if healthcare systems are to reap the societal benefits promised by the implementation of electronic health records (EHRs). Health information technology (HIT) interoperability refers to the ability of multiple EHR systems and software applications to communicate, share, and use data. Considering the geographical spread of healthcare infrastructure and the globalization and corporatization of the healthcare sector, it is a well-established fact that interoperability is key to the successful deployment of a competitive healthcare landscape. Various studies have explored the potential of interoperable blockchain networks in the healthcare sector, and they were largely of the view that interoperability is the key to healthcare sustenance [15] [16] [17].
The objectives of this study are to propose a framework for integrating heterogeneous blockchains in a federation and to evaluate the performance of inter-blockchain data transfer. The proposed framework seeks to resolve the inefficiencies and lack of interoperability in existing healthcare blockchains by proposing a CCC protocol. This protocol is designed to support transactions between diverse blockchains in a federation, thereby enabling inter-blockchain data transfer within the federation. By integrating multiple blockchain networks, the proposed framework establishes an open system that promotes interaction between devices and users across blockchain boundaries. The proposed solution considers several assumptions, including (a) the federation is comprised of individual blockchain networks that possess unique architectures, platforms, business logic, and consensus protocols, and operate independently of one another; (b) the blockchain networks require a prior registration in the federation; (c) each blockchain model fully controls its assets and information; (d) the interoperability solution ought to refrain from altering the state of the affiliated network; and (e) the source and target networks ought not to be acquainted with the architecture of the connected network. This study makes the following contributions:

- Proposing a novel CCC protocol for integrating diverse blockchain networks through the use of global smart contracts that are activated by transaction-based triggering technique.

- Designing a global smart-contract framework encompassing conversion, connection, and transfer contracts to promote inter-blockchain transactions.

- Proposing a conversion contract that is capable of efficiently converting transactions from various local formats to a unified, standardized format suitable for the target blockchain network, thereby enhancing interoperability.

- Validating the practical applicability of the CCC protocol by integrating Ethereum and Hyperledger Fabric (HLF) healthcare networks, providing evidence of its usefulness in real-world situations.

- Assessing the security, performance, and query processing time of the CCC protocol using a rigorously designed evaluation model, providing vital information on its effectiveness and scalability in facilitating seamless CCC and data exchange.

The rest of the paper is organized as follows: Section 2 describes the related work relevant to our study. In Section 3 we present the proposed solution, followed by Section 4 to provide performance evaluation. In Section 5 the experimental setup and results are discussed. Section 6 concludes the paper.

2. Related Work

This section summarizes the related work done in the field of blockchains interoperability. Interoperability among blockchain networks is the concept of triggering the smart contract across heterogeneous blockchain networks [18]. In the literature various mechanisms are used for inter-blockchain communication, including notary schemes [19] [20] [21] [22] [23] [14] [18] [24], sidechain solutions [25] [26] [27] [28] [29] [30], smart contract-based solutions [17] [31] [32] [33] [34] [35], bridging solutions [36] [37] [38] [39], and blockchain router solutions [13] [40] [41]. The details of each scheme are presented in [16].
The impact of blockchain technology on the healthcare industry has been signified by enabling the integration of various healthcare stakeholders into a distributed network. However, many healthcare blockchains currently operate in isolation, and ongoing research is focused on developing CCC protocols for the sharing of EHRs across healthcare networks. The work reported in [42] provides an initial practical implementation of homogeneous blockchain integration using HLF networks. This model achieves cross-blockchain communication in three stages: 1. interaction between smart contracts in the same channel and network, 2. interaction between smart contracts in different channels but the same network, and 3. interaction between smart contracts in different networks. The Node-RED framework is utilized as a mediator. However, the solution is HLF architecture-based and could be applied to other platforms in a federation. An application-level integration is proposed in [15] for sharing EHRs of patients registered in independent blockchain networks. This work methodology involves token generation, EMR document retrieval, verification, and transfer of records via an off-chain mechanism utilizing the Ethereum network. However, the implementation details have not been tested on other platforms for a general-purpose solution. Similar work is reported in [43] at the application level for integrating blockchain networks in two stages: information query and state change. This model assumes that the corresponding blockchain systems have smart contract capabilities, but the smart contract design

and compatibility are not mentioned, nor does it provide a real-world implementation challenge. The research, reported in [44], introduces a blockchain architecture based on Autonomous Systems (AS) that enables interoperability through trusted gateways utilizing TEE and atomic swapping with threshold signatures. However, the work does not provide empirical validation or experimental results to assess the latency of communication processes. Another study, [18], presents a TEE-based approach for interoperability in collaborative manufacturing scenarios, involving the federation of blockchains through inter-blockchain smart contracts to facilitate coordinated information exchange between companies in a manufacturing supply chain. The model was tested with heterogeneous networks integration but achieved high latency due to potential performance bottlenecks associated with secure communication protocols and TEE execution.

Through an extensive review of the literature, it becomes evident that previous studies primarily focus on integrating homogeneous networks. However, the pioneering work addressing the integration of heterogeneous networks encounters a significant challenge in the form of heightened latency during data transfer across diverse networks. Given the context of the healthcare domain, where swift and seamless data transmission is paramount, latency emerges as a critical factor warranting thorough consideration. In light of these limitations, this study proposes a layer-1 solution using a unified integrated approach for integration networks deployed on different blockchain platforms. The proposed solution aims to address the challenges of heterogeneous network integration in a federation.

3. Proposed Methodology

The proposal entails the development of an integration framework for blockchains that employs a global smart contract-triggering solution for facilitating the sharing of EHRs across diverse networks within a blockchain federation. Figure 1 illustrates a high-level overview of the proposed method, and below we describe in detail the framework's major elements and examples of the EHRs sharing steps. In the proposed integration model, two healthcare-based blockchain networks are deployed in a federation, B1 and B2. We assume that a patient currently visiting B1 has an appointment with a caregiver (CG) and has a previous record of his medical treatment in B2. The CG at B1 needs access to his previous record from B2 for a complete history and diagnosis. The CG at B1 initiates a request to B2 to retrieve the patient's record on behalf of the patient. In the integration process, the patient ID is used instead of the patient public key (PK) as each network generates its own PK for the same patient in the federation. However, the patient ID is identical throughout the federation. The source blockchain (B1) attempts to trigger the smart contract at the target blockchain (B2) for the patient's record retrieval via the global smart contract and the CCC protocol. The target blockchain processes the query transaction generated by B1 and transfers the needed EHR of the patient to B1. Figure 2 shows a step-by-step execution sequence of the proposed CCC protocol, initiating a query transaction from the source blockchain to the target blockchain.

A. *Blockchain Interoperability*

Interoperability is the possibility of exchanging or sharing assets across different blockchains networks. In this study, we use a unified integrated interoperability approach [42] for CCC between heterogeneous blockchain networks. First, we assume that both networks are registered in a federation running in a state/county. Healthcare blockchains are implemented in private or consortium models due to the security concerns associated with medical data. According to [28], if one blockchain network accepts transactions from another, then they are interoperable with each other. In doing so, we propose global smart contracts for CCC. As shown in Fig. 3, both networks are developed using distinct platforms and with different business logic and smart contracts. However, being a part of the federation, the global smart contracts are unified in all blockchain networks of the federation and are responsible for the connection to the communication module and establishing the communication link between the source and target networks.

B. *Global Smart Contract*

Smart contracts are programs designed for specific tasks in the blockchain network and are triggered when predefined conditions are met in the network. In this study, two types of smart contracts are used: local and global. Local smart contracts are designed specifically to meet the requirements of the blockchain application domain with specific business logic and are executed locally in the network. On the other hand, global smart contracts are unified contracts that must be deployed on each blockchain network, as depicted in Figure 3. These contracts are designed to interoperate and share data across multiple networks in a federation. The proposed global smart contract is comprised of three modules: conversion contracts, connection contracts, and transfer contracts. The details of each of the smart contracts are discussed in the following subsections.

1) *Conversion Contract*

The conversion contract within the framework of the global smart contract facilitates the acceptance of transactions in a local format native to the underlying platform, subsequently transforming the transactions into a uniform format harmonious with the target network. The proposed uniform transaction format is as follows:

From the sender (B1 to B2)

$$Txn < \ P_{id}, D_{PK}, D_{add}, \text{P\_CF, Timestamp, Sig} >$$

From the receiver (B2 to B1)

$$Txn < \ P_{id}, D_{PK}, \text{Hash(EHR), Timestamp, Sig}>$$

where P_{id} is the patient's ID, D_{PK} is a caregiver's (CG) public key, P_CF is the patient's consent form, Sig is for the digital signature. The transaction is subjected to digital

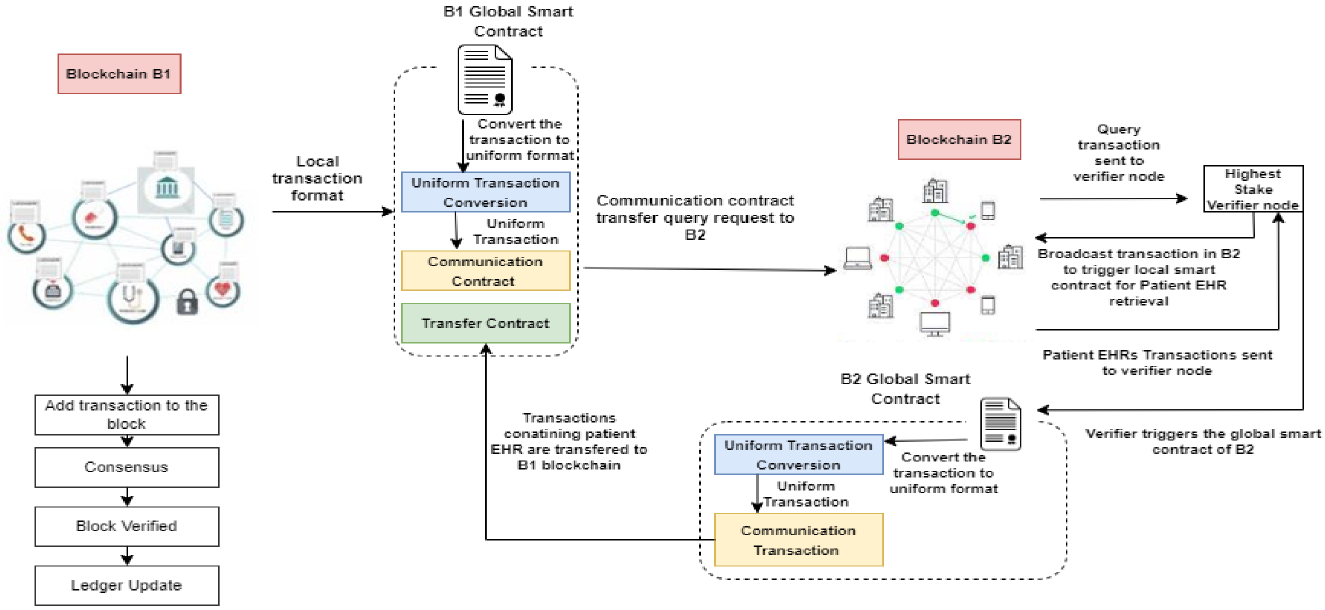
B1 Global Smart Contract
Blockchain B1
Convert the transaction to uniform format
Local transaction format
Uniform Transaction Conversion
Uniform Transaction
Communication Contract
Transfer Contract
Communication contract transfer query request to B2
Blockchain B2
Query transaction sent to verifier node
Highest Stake Verifier node
Broadcast transaction in B2 to trigger local smart contract for Patient EHR retrieval
Patient EHRs Transactions sent to verifier node
B2 Global Smart Contract
Verifier triggers the global smart contract of B2
Add transaction to the block
Consensus
Block Verified
Ledger Update
Transactions conatining patient EHR are transfered to B1 blockchain
Uniform Transaction Conversion
Convert the transaction to uniform format
Uniform Transaction
Communication Transaction

Figure 1. Workflow of proposed cross-chain communication model

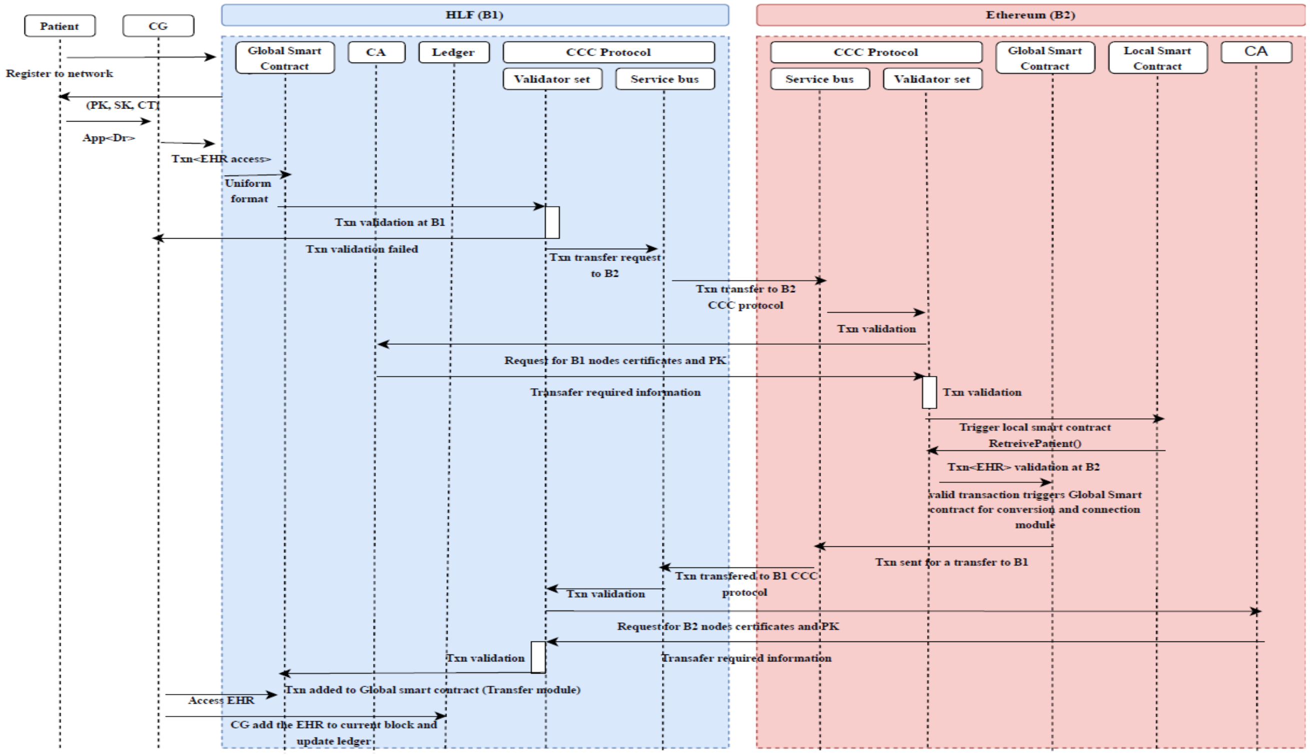
HLF (B1)
Ethereum (B2)
Patient
CG
Global Smart Contract
CA
Ledger
CCC Protocol
Validator set
Service bus
CCC Protocol
Service bus
Validator set
Global Smart Contract
Local Smart Contract
CA
Register to network
(PK, SK, CT)
App<Dr>
Txn<EHR access>
Uniform format
Txn validation at B1
Txn validation failed
Txn transfer request to B2
Txn transfer to B2 CCC protocol
Txn validation
Request for B1 nodes certificates and PK
Transafer required information
Txn validation
Trigger local smart contract RetreivePatient()
Txn<EHR> validation at B2
valid transaction triggers Global Smart contract for conversion and connection module
Txn sent for a transfer to B1
Txn transfered to B1 CCC protocol
Txn validation
Request for B2 nodes certificates and PK
Transafer required information
Txn validation
Txn added to Global smart contract (Transfer module)
Access EHR
CG add the EHR to current block and update ledger

Figure 2. Execution sequence of proposed inter-blockchain communication model

signature authentication utilizing the cryptographic private key associated with CG. Upon receipt, the target network verifies the integrity of the digital signature using the complementary public key corresponding to CG. The patient consent form ensures that the retrieval of the patient's record from the target network is conducted with explicit consent from the patient or their designated representative. Further, the patient consent form is digitally signed by the patient's private key (private key generated at the target network). Subsequently, this digital signature is verified by the target

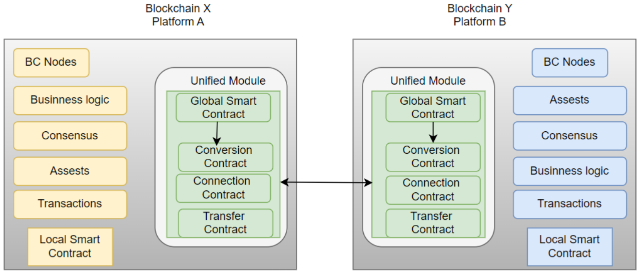

Figure 3. Architectural components of blockchains in a federation

network through the patient's corresponding public key. Upon successful verification of the signature, the target network initiates the execution of a local smart contract tasked with retrieving the patient's EHR. As part of this retrieval process, the patient's EHR is hashed using the SHA256 algorithm before being appended to the transaction. This ensures data integrity and security throughout the transmission and retrieval process within the blockchain networks.

2) *Connection Contract*

The connection module enables communication among the connected networks through the utilization of the certification authority (CA) address inherent to the target network. Activation of this module is instigated by the receipt of the uniform transaction, thereby effectuating the establishment of network connections and facilitating the CCC protocol for the transfer of queries and patient records amidst the interconnected networks.

3) *Transfer Contract*

The transfer contract is designed to retain the transaction obtained from the target network, encompassing the EHR data of the patient. This data is encrypted by the target network using the PK of the CG originating from the source network.

In Algorithm 1 and Algorithm 2, we outline a detailed step-by-step process for triggering the global smart contract in both the source and target networks, respectively, highlighting the essential role these contracts play in our interoperability model. A list of abbreviations used in the algorithms is provided in Table 1.

C. *Cross-Chain Communication Protocol*

A CCC protocol enables interoperability between independent blockchain networks. This eliminates the need for any third-party intermediary, such as an exchange platform, thereby enabling network participants to share data across different platforms within a federation. This gives individuals more control as they navigate data/assets and contribute to the decentralization of the entire ecosystem. The proposed CCC protocol does not cause a direct state change in the external/target network; instead, it executes a series of functionalities (smart contract) within the external network that could lead to changing the state in the source

Algorithm 1 Healthcare blockchain federation global smart contracts triggering (Source network)

```
Require: $(B_1, B_2, ..., B_n)$, $P_{pk}$, $DiB_1$
Ensure: $(EHR)Pi$
$Di_{B1} \leftarrow$ Transaction Initiator
$Di_{B1} \rightarrow Txn < Txn\_Type, P_{pk}, Di_{pk}, P\_CF, DS(Di_{B1}) >$
if $Txn\_Type ==$ ”$intra - blockchain$” then
    $Txn \rightarrow LSC_{B1}$
else if $Txn\_Type ==$ ”$inter - blockchain$” then
    $Txn \rightarrow GSC_{B1}$
    PROCEDURE Conversion_Contract($Txn$)
    $Txn \rightarrow$Uni_Txn<$P_{ID}, (Dpk)_{B1}, P\_CF, DS(Di_{B1})$ >
    return $Uni\_Txn$
    PROCEDURE Connection_Contract($Uni\_Txn$, $(S\_CA)add$, $(T\_CA)add$)
    Create_Connection($(S\_CA)_{B1} \rightarrow (T\_CA)_{B2}$)
    $(S\_CA)_{B1} < Uni\_Txn > \rightarrow (T\_CA)_{B2}$
end if
```

Algorithm 2 Healthcare blockchain federation global smart contracts triggering (Target network)

```
Require: Uni_Txn
Ensure: $(EHR)Pi$
$(T\_CA)_{B2} \leftarrow$ Receive Transaction
# Validators Selection
for $V$ in $V\_Set$ do
    $V_{B2} \leftarrow$ max_Stake($V\_Set$)
end for
$(T\_CA)_{B2} < (Txn)_{B1} > \rightarrow V_{B2}$
$V_{B2} < (Txn)_{B1} > \rightarrow$ Validation
if Validation == Success then
    $V_{B2} \leftarrow$ Transaction Initiator in $B_2$
    $V_{B2} < (Txn)_{B2} > \rightarrow LSC_{B2}$
    $V_{B2} \leftarrow (EHR)P_{ID}$
    $V_{B2}$ adds $(EHR)P_{ID}$ to $(Txn)$
    $V_{B2} < (Txn)_{B2} > \rightarrow GSC_{B2}$
    PROCEDURE Conversion_Contract($Txn$)
    PROCEDURE Connection_Contract($Uni\_Txn$, $(B_1\_CA)add$, $(B_2\_CA)add$)
    PROCEDURE Transfer_Contract($Uni\_Txn$)
    $LSC_{B1} \leftarrow (EHR)P_{ID}$
else
    discard $(Txn)B_1$
end if
$Di_{B1}$ Update ledger $B_1$
$Appointment = NULL$
```

TABLE I. List of notations

Notation	Description
D^i_{B1}	Doctor node at B1
Txn	Transaction
Txn _Type	Transaction type
P_{pk}	Patient public key
D_{pk}	Doctor public key
P_{ID}	Patient ID
$(T\_CA)add$	Target network CA address
CH_i	Chain code
P_CF	Patient consent form
DS	Digital signature
LSC_{B1}	Local smart contract of B1
GSC_{B1}	Global smart contract of B1
Uni_Txn	Uniform transaction format
$(S\_CA)add$	Source network CA address
V_{B2}	B2 validator

network. Within the scope of this research, the CCC protocol activates the RetrivePatientData() module of the smart contract in the target network. Furthermore, modification of EHRs in an external blockchain is not the focus of this investigation. The CG at B1 prepares a transaction proposal for initiating a query transaction to access the Pi record from an external network as,

$$T_{xn} < P_{PK}, D_{PK}, D_{add}, P\_CF, Txn\_type, Txn\_id, CH_i, \\ Btarget = value, (T\_CA)add, Timestamp, Sig >$$

The Txn_type = interblockchain triggers the global smart contract. Btarget refers to the target network platform. If Bsource Btarget, then Btarget=value invokes the conversion module to convert the local transaction format to a uniform standard format. The P_{PK} is exchanged by the P_{id} since each network in the federation generates a unique public/private key pair for the network participants. In the proposed framework, we are using the P_{id} as it is uniform within the federation. After converting the transaction to a uniform format, the connection contract establishes the connection to the target network using the Btarget-add. All blockchain platforms have some common functionalities, such as verifying the digital signatures of the submitted transactions, a consensus algorithm for finalizing the transactions, and block generation. Running these functionalities on an external network is challenging for a federation of independent networks. In the proposed model, transactions are deployed in an external network, where each network runs its own business logic, consensus algorithm, and block generation. An external network cannot play a role in the internal functionalities of any network. However, it is crucial to verify that the transaction validation is performed at both ends. Within a single network, a hierarchical public key infrastructure (PKI) was used to speed up the verification process using multiple CAs in the network. Each healthcare entity has a CA with a trusting relationship with the network nodes within the entity. A single root CA in the network has a trust relationship with all the CAs in the network. In this hierarchy of trust, the verification is performed as follows:

$$CA_1 \rightarrow Bn_a, Bn_b, Bn_c, \ldots\ldots \tag{1}$$

$$CA_2 \rightarrow Bn_1, Bn_2, Bn_3, \ldots\ldots \tag{2}$$

where CA_1 verifies the digital signatures of blockchain nodes (Bn_a, Bn_b, Bn_c) and CA_2 verifies those of blockchain nodes (Bn_1, Bn_2, Bn_3). If CA1 has a trust relationship with CA2, then the nodes verified by both CAs have a trust relationship with each other as follows:

$$(Bn_a, Bn_b, Bn_c) \rightarrow (Bn_1, Bn_2, Bn_3) \tag{3}$$

For transaction verification across the blockchains, we used a set of validators in the CCC protocol that verifies the digital signatures of the entities that initiate transactions from one network to another. To validate the transactions of both networks, the validator set must be trusted nodes and participants in networks 1 and 2. In this scenario, the validators of the CCC protocol validate the digital signature of both network participants, i.e.,

$$CC_V = \{v1, v2, v3, \ldots\ldots\} \tag{4}$$

$$\{v1, v2, v3, \ldots\ldots\} \subseteq (nw1, nw2) \tag{5}$$

$$CC_V \rightarrow CA\_nw1, Vs\_nw2 \tag{6}$$

where CC_V is the validator set comprising validator nodes v1, v2, v3, etc. The validator set has a trust relationship with the CA of network 1 and the validators of network 2 (CA_nw1, Vs_nw2), and the CAs and validators of both networks have a trust relationship with the local CAs/validators of their network as:

$$CA\_nw1 \rightarrow CA_1, CA_2, CA_3, \ldots\ldots \tag{7}$$

If (1) and (2) are for network 1, then from (6) and (7) we have CC_V trusts the blockchain nodes of network 1, i.e.,

$$CC_V \rightarrow CA_1, CA_2, CA_3, \ldots\ldots \tag{8}$$

$$CC_V \rightarrow \{Bn_1, Bn_2, Bn_3\} and \{Bn_a, Bn_b, Bn_c\} \tag{9}$$

Similarly, for network 2, the validator nodes have a trust relationship with their blockchain nodes as

$$Vs\_nw2 \rightarrow b_1, b_2, b_3 \tag{10}$$

Then (12) can be written as

$$CC_V \rightarrow \{Bn_1, Bn_2, Bn_3\}\{Bn_a, Bn_b, Bn_c\}\{b_1, b_2, b_3\} \tag{11}$$

Once the verification process is completed at the target network, a verifier node is selected to trigger the smart contract of the network to access the requested patient record. In the current scenario, a verifier node is selected from a set of verifiers in a proof-of-stack consensus as, Vmax_stake[v1, v2, v3,. . . .vn]. The highest stake verifier node triggers the RetrievePatient() smart contract in the target network to access the patient's record.

4. PERFORMANCE EVALUATION

In this section, we assess the performance of the proposed inter-blockchain data transfer in terms of (i) security, (ii) the individual performance of each network (throughput, latency, and success rate), and (iii) the CCC elapsed time for query processing.

A. *Security Assessment*

The proposed model provides an interoperable solution between independent blockchains. The security assessment of our proposed model depends on the secure configuration of the connected blockchain network, which results in a secure CCC protocol. In this model, each blockchain is responsible for validating the transactions locally and using hierarchical PKI [17], validation across the networks is achieved by the trust relationship between the validator nodes in the federation. Furthermore, verifiers may ask to share the public key of the external blockchain validator to establish a trusting relationship for transaction validation. In the proposed model, network participants do not share private or sensitive information with the external network during the communication process because transaction validation and consensus are performed locally and depend on the secure configuration of the underlying network.

Our proposed model does not deploy third-party/external validators in the CCC protocol; each network deploys its validators in the CCC protocol depending on the availability and reputation of the validators in both networks. In the case of HLF, a CA was deployed to validate the certificates of the participants to validate transactions. In the Ethereum network, a set of validators is used for the CCC protocol based on their stake, and consensus between them is achieved using the same consensus algorithm adopted in the network.

B. *Network Performance*

To ensure the effectiveness of this integration, the performance of each network within the federation was rigorously assessed using key performance indicators such as throughput, latency, and transaction success rate. Throughput is the number of transactions committed to the network, latency is the time delay between the transaction submitted to the network and transaction confirmation, and send rate is the number of transactions sent to the network. This evaluation process is crucial because it highlights the significant influence of an individual network's performance on the execution of the CCC protocol in each network.

C. *Cross-Chain Communication Elapsed Time*

The elapsed time (ET) of the CCC protocol quantifies the duration starting from the initiation of a query transaction in the source network (T_S) to the receipt of a response from the target network (T_R), i.e.,

$$ET = T_R - T_S \tag{12}$$

Cross-chain exchange necessitates the validation of transactions originating from a source network by a target network. Consider a transaction, denoted as Txn, initiated at B1 to solicit a patient's EHR from B2. Subsequently, the ET of the CCC protocol is computed as the set of operations executed at B1 and B2, in conjunction with the round-trip communication time (CT) from B1 to B2 and vice versa, i.e.,

$$\begin{aligned} ET = {} & V_{B1}(Txn) + CT_{(B1,B2)(B2,B1)} + V_{B2}(Txn) + \\ & SC_{B2}(Txn) + V_{B2}(R\_Txn) + V_{B1}(R\_Txn) \end{aligned} \tag{13}$$

In the described scenario, $V_{B1}(Txn)$ represents the temporal interval necessary for transaction validation operations at B1, whereas $V_{B2}(Txn)$ signifies the duration required for transaction validation procedures at B2. Additionally, $SC_{B2}(Txn)$ denotes the timeframe essential for initiating a smart contract at B2 to access the EHR pertinent to the query transaction originated from B1. Subsequently, R_Txn denotes the response transaction encompassing the hash value of the patient record solicited by B1, with $V_{B2}(R\_Txn)$ representing the temporal duration necessary for validating the response transaction at B2, and $V_{B1}(R\_Txn)$ denoting the equivalent validation duration at B1. Notably, $V_{B2}(Txn)$ and $V_{B1}(R\_Txn)$ represent transactions validated by external networks, thereby necessitating the verifiers of the CCC protocol to request the PK and certificates of validation from external networks to facilitate verification processes. This process aims to nurture a trusting relationship among the validators originating from both networks, thereby safeguarding the integrity and reliability of the validation mechanisms utilized across interconnected networks.

5. Experiments

The proposed CCC protocol was implemented using two independent networks, Ethereum [45] [46] [47] and HLF [48]. Ethereum was utilized as a constrained test network to authenticate the proposed interoperability solution which is integrated with the consortium test network of HLF. Hyperledger Caliper was used for the performance evaluation of the integrated networks [49]. The experimental setup, aimed at establishing a test environment conducive to the inter-blockchain communication concept, adhered to the subsequent hardware specifications: (1) Two Core CPU (Intel (R) Core TM i5-4570 CPU @ 3.20 GHz), (2) Ubuntu OS (20.04.1 (TS)).

A. *Results and Discussion*

In this subsection, we present the performance evaluations of Ethereum and HLF private networks using Hyperledger Caliper. An analysis was conducted to evaluate the individual performances demonstrated by the two networks and to discern any potential impact on the outcomes of inter-blockchain communication. Hyperledger Caliper served as the benchmark configuration, wherein five worker nodes were established, and each experiment was executed five times to derive an average result. Figure 4 shows the average throughput performance by Ethereum and HLF for a transaction rate of 50 transactions per second (TPS).

Individual performance indicators are analyzed for the Ethereum and HLF performance comparison in terms of

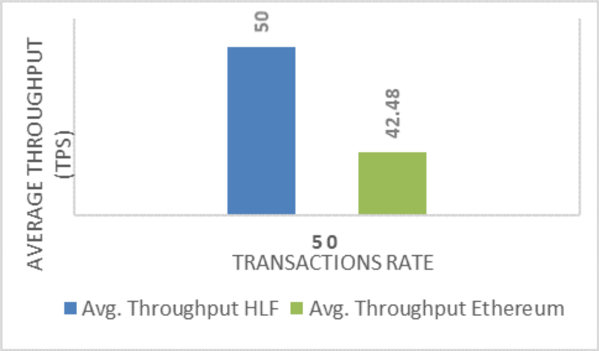

Figure 4. Throughput comparison of Ethereum and HLF

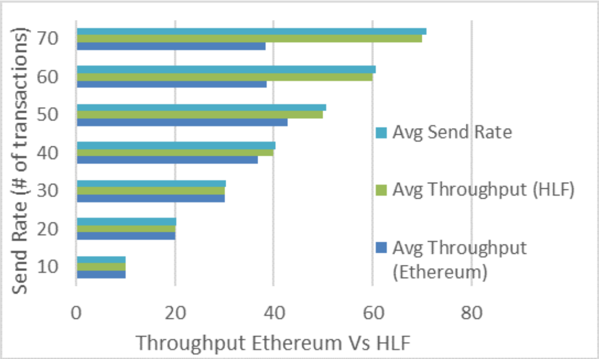

Figure 5. Transacion send rate vs. avg. throughput (Ethereum) and avg. throughput (HLF)

throughput, latency, and send rate with increasing transaction rates from 10 to 70 TPS. Figure 5 shows the throughput performance of both networks. A gradual increase in the throughput of both networks was noted as the transaction rate increased from 10 to 50 TPS. However, Ethereum throughput decreases as the transaction rate reaches and exceeds 50 TPS, which reflects the computational complexity of the Ethereum network for increased transaction load as compared to HLF.

Figure 6 shows the latencies of both networks, where the Ethereum latency increased faster than the HLF latency with increasing transaction load in the network. Concluding the performance comparison of HLF and Ethereum, the HLF network provides a higher throughput and lower latency than the Ethereum network. This comparison is significant for the query processing time in both networks of a federation.

Next, we discuss the results of implementing the proposed inter-blockchain communication model. A unified integrated approach was used to integrate the HLF and Ethereum networks. Within a federation, each blockchain is required to deploy the unified module. In this setup, we used the Hyperledger Cactus [50] for deploying the unified module in the federation. Hyperledger Cactus is an open-source project hosted by the Linux Foundation under the Hyperledger umbrella. The Cactus service bus and the Cactus test node are used to deploy the proposed

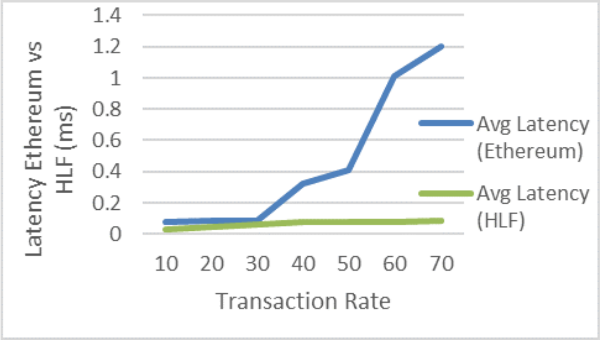

Figure 6. HLF and Ethereum latencies

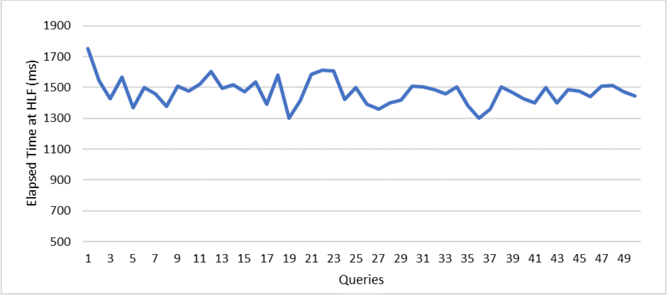

Figure 7. Inter-blockchain record access elapsed time

CCC protocol in both networks. The Cactus test node is utilized to initiate query transactions from the source blockchain. It acts as a bridge between the source and target networks, facilitating communication between them. The test node is responsible for initiating transactions, verifying their authenticity, and forwarding them to the service bus for further processing. The Cactus service bus functions as a communication channel for transactional exchanges between the source and target networks, guaranteeing the secure and dependable transmission of transactional data. This facilitates the interoperability between the two blockchain networks. Additionally, the service bus is responsible for managing the routing, validation, and delivery of transactions, ensuring their efficient delivery to their designated endpoints. Together, the Cactus test node and the Cactus service bus form a robust infrastructure for implementing the CCC protocol, enabling seamless inter-blockchain communication and data exchange between HLF and Ethereum networks.

The CG at source network (HLF) initiates a query transaction of the patient's EHR from the target network (Ethereum). As illustrated in Figure 7, the ET for the query transaction encompasses both the CT and the processing time required for the query at the target blockchain. The ET is determined using the formula specified in Equation (13). It is noteworthy that the initial ET for query 1 surpasses that of subsequent queries. This discrepancy is attributed to the initial connection establishment process with the target network and subsequent verification procedures. After the establishment of the connection, the ET exhibits a decline,

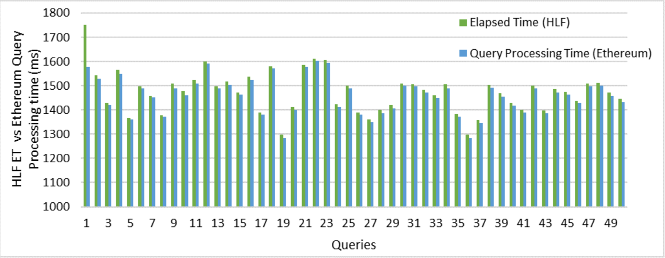

Figure 8. HLF elapsed time paired with query processing time at Ethereum network

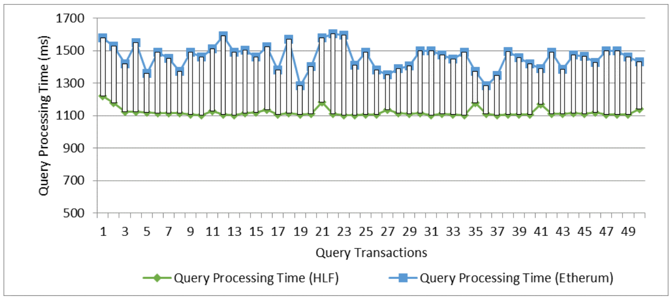

Figure 9. Query processing comparison at Ethereum and HLF networks

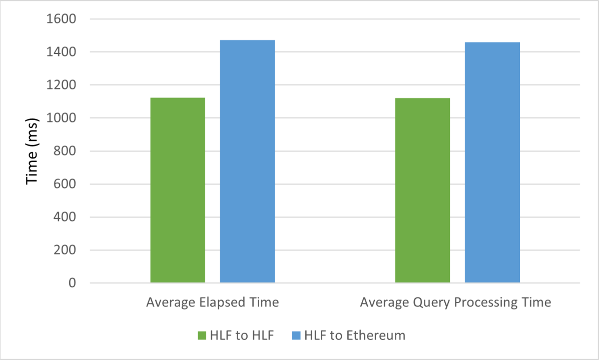

Figure 10. Comparison of elapsed time and query processing time between Ethereum and HLF

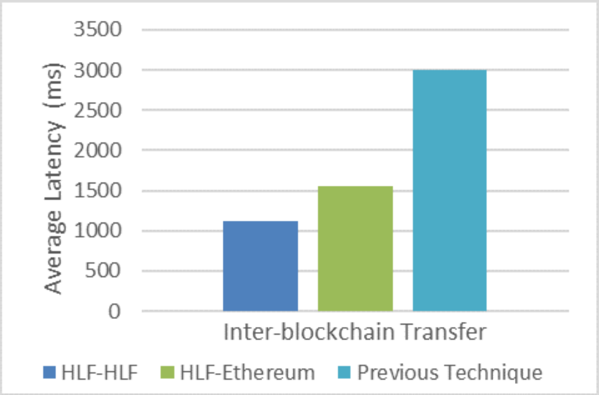

Figure 11. Average latency comparison at source network

with fluctuations in ET primarily attributable to variations in query processing times at the target network. The evaluated query processing times specific to Ethereum are depicted in Figure 8, compared with the corresponding ET. A comparative analysis of query processing times between the two networks, illustrated in Figure 9, underscores the superior performance of the HLF network, thereby exerting a significant influence on the ET within the source network.

Figure 10 provides a comparative analysis of the inter-blockchain communication processes within both homogeneous and heterogeneous network configurations within a federation. Notably, the average ET observed for transactions between HLF networks was notably lesser in comparison to transactions bridging between HLF and Ethereum networks, primarily due to the relatively inferior performance exhibited by the Ethereum network. This discrepancy is elucidated by the comparatively prolonged query processing times evident within the Ethereum network when contrasted with those observed within the HLF network. Consequently, this variation contributes to the extended ET experienced within the HLF network during communication exchanges with the Ethereum network.

In this study, we conducted a comparative analysis between our novel CCC protocol and the framework presented in a previous work [18]. The authors of the previous study utilized a relay scheme based on Trusted Execution Environments (TEE) to address blockchain interoperability within the domain of supply chain management. However, the inherent complexity associated with TEE-based solutions introduces challenges, particularly in terms of implementation intricacies and the potential performance overhead attributed to secure communication protocols like Transport Layer Security (TLS). Consequently, this complexity led to increased latency, that was deemed acceptable in the supply chain context. In contrast, the domain of healthcare places a significant emphasis on minimizing latency due to its critical nature. Although these two domains are not directly comparable, relevant literature is scarce for a more precise comparison. Nevertheless, overcoming this challenge, our comparative analysis revealed a notable enhancement in latency performance with our proposed CCC protocol when compared to the framework proposed in [18], as demonstrated in Figure 11.

In summary, the inaugural connection established with the Ethereum network exhibits an 18% higher rate compared to subsequent query transactions originating from HLF to Ethereum. This discrepancy is further exacerbated by a 3% increase relative to the initial connection established within HLF-to-HLF interactions. Moreover, the average ET observed from HLF to Ethereum transactions registers a 26% increase when contrasted with HLF-to-HLF transactions. This amplified duration is attributable to the performance disparity within the Ethereum network, which experiences a 15% decrease in TP efficiency in comparison to the HLF network's TP. Consequently, the experimental findings underscore the dependence of ET on the query processing time specific to the target blockchain network. Moreover, our proposed protocol exhibited a latency improvement of 78% for homogeneous integration and 52% for heterogeneous integration compared to [18].

The optimized latency efficiency attained represents a paramount advancement within the multifaceted healthcare sector. This breakthrough not only serves to streamline the intricate process of data sharing but also facilitates the seamless accessibility and utilization of pivotal patient data across diverse healthcare blockchain networks. As a result, this promotes cooperative partnerships among stakeholders, improving not just treatment approaches but also driving advancements in research initiatives and the comprehensive provision of patient care.

Finally, we identify the limitations of this study. Blockchain addresses are typically represented by public keys, which are utilized to request EHR within the network. However, in this study, an alternative method is employed whereby the patient's identification, such as their national identity card number or citizenship number, is utilized to initiate EHR requests from an external blockchain. Each blockchain network generates a unique pair of public and private keys specific to its network, ensuring confidentiality across external networks. Therefore, the adoption of patient ID, which remains consistent within a country or state, offers a practical solution. Upon transferring the transaction to the target network, the patient ID is subsequently substituted with the patient's public key generated within the underlying network. The employment of separate key pairs within a federation introduces complexities for patients in managing multiple keys. Nevertheless, this challenge can be effectively addressed by implementing a unified key pair across the federation. Such an approach not only streamlines the process but also serves to significantly enhance the efficiency of record transmission across interconnected networks.

The proposed framework is implemented using HLF and Ethereum only, due to the complexity of blockchain networks and time constraints associated with this research. However, we aim to expand our experimentation in the future by incorporating additional blockchain networks into the federation.

6. Conclusion

Blockchain interoperability is an emerging field of research that allows independent blockchains to share assets and data within a federation. In this research, we propose a unified integrated approach by implementing a global smart-contract triggering method for CCC across the blockchain networks of a federation. In this approach, global smart contracts are strategically deployed as unified modules within federation networks. These global smart contracts include a conversion module that standardizes local transactions into a uniform format, thereby ensuring compatibility across external networks. Following this conversion, a local smart contract for the external network is triggered for accessing patient records. We compared the integration of homogeneous and heterogeneous networks and concluded that the query processing time of the target network had a major impact on the performance of the overall integration process. Our proposed protocol exhibited a latency improvement of 78.09% for homogeneous integration and 52.63% for heterogeneous integration compared to [18].

In future research endeavors, our objective is to investigate the formulation of a unique public/private key pair for patients residing in independent networks within a federation. This will help patients maintain a single key pair across the federation and the CCC protocol enhancement for searching patients' registration in the federation. Additionally, we aim to explore machine learning algorithms to efficiently locate patient records distributed across external networks, thereby bolstering the performance of our CCC protocol.

Further investigation is warranted to expand the implementation of our proposed model to encompass other blockchain networks. This comprehensive approach will facilitate a comparative assessment of the performance of the CCC protocol within the federation, offering insights into its efficacy and scalability across varied network environments.

Acknowledgment

This research is funded by Zayed Center for Health Sciences, the United Arab Emirates University Grant number 31R180 and the sponsors of the 4th Forum for Women in research (QUWA, Sustainable Women's Empowerment in Research Innovation held at the University of Sharjah, UAE): Abu Dhabi National Oil Company (ADNOC), Emirates NBD, Sharjah Electricity Water Gas Authority (SEWA), Technology Innovation Institute (TII) and GSK. We would like to extend our thanks to Mr. Juhar Abdella from RMIT for his technical support.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] J. Hathaliya, P. Sharma, S. Tanwar, and R. Gupta, "Blockchain-based remote patient monitoring in healthcare 4.0," in *2019 IEEE 9th international conference on advanced computing (IACC)*. IEEE, 2019, pp. 87–91.

[3] K. Shuaib, H. Saleous, K. Shuaib, and N. Zaki, "Blockchains for secure digitized medicine," *Journal of personalized medicine*, vol. 9, no. 3, p. 35, 2019.

[4] H. Subramanian, "Decentralized blockchain-based electronic marketplaces," *Communications of the ACM*, vol. 61, no. 1, pp. 78–84, 2017.

[5] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, pp. 1–8, 2016.

[6] B. Shen, J. Guo, and Y. Yang, "Medchain: Efficient healthcare data sharing via blockchain," *Applied sciences*, vol. 9, no. 6, p. 1207, 2019.

[7] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, "Healthsense: A medical use case of internet of things and blockchain," in *2017 International conference on intelligent sustainable systems (ICISS)*. IEEE, 2017, pp. 486–491.

[8] V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health informatics journal*, vol. 25, no. 4, pp. 1398–1411, 2019.

[9] F. Hashim, K. Shuaib, and F. Sallabi, "Medshard: Electronic health record sharing using blockchain sharding," *Sustainability*, vol. 13, no. 11, p. 5889, 2021.

[10] ——, "Performance evaluation of blockchain consensus algorithms for electronic health record sharing," in *2021 Global Congress on Electrical Engineering (GC-ElecEng)*. IEEE, 2021, pp. 136–143.

[11] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Computing Surveys (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021.

[12] Z. Chen, Y. Zhuo, Z.-B. Duan, and H. Kai, "Inter-blockchain communication," *DEStech Transactions on Computer Science and Engineering http://dx. doi. org/10.12783/dtcse/cst2017/12539*, 2017.

[13] L. Kan, Y. Wei, A. H. Muhammad, W. Siyuan, L. C. Gao, and H. Kai, "A multiple blockchains architecture on inter-blockchain communication," in *2018 IEEE international conference on software quality, reliability and security companion (QRS-C)*. IEEE, 2018, pp. 139–145.

[14] 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.

[15] 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. 87 777–87 791, 2021.

[16] F. Hashim, K. Shuaib, and F. Sallabi, "Connected blockchain federations for sharing electronic health records," *Cryptography*, vol. 6, no. 3, p. 47, 2022.

[17] 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, 2017, pp. 73–81.

[18] P. Bellavista, C. Esposito, L. Foschini, C. Giannelli, N. Mazzocca, and R. Montanari, "Interoperable blockchains for highly-integrated supply chains in collaborative manufacturing," *Sensors*, vol. 21, no. 15, p. 4955, 2021.

[19] M. Borkowski, M. Sigwart, P. Frauenthaler, T. Hukkinen, and S. Schulte, "Dextt: Deterministic cross-blockchain token transfers," *IEEE access*, vol. 7, pp. 111 030–111 042, 2019.

[20] S. Yang, H. Wang, W. Li, W. Liu, and X. Fu, "Cvem: A cross-chain value exchange mechanism," in *Proceedings of the 2018 International Conference on Cloud Computing and Internet of Things*, 2018, pp. 80–85.

[21] (2024) Icon documentation. Accessed: Jan. 25, 2023. [Online]. Available: https://docs.icon.community/

[22] (2024) Crypto solutions for business — ripple. Accessed: Dec. 25, 2023. [Online]. Available: https://ripple.com/

[23] Metronome: The built-to-last cryptocurrency. Accessed Dec. 05, 2022. [Online]. Available: https://www.metronome.io/

[24] Cosmos: The internet of blockchains. Accessed Dec. 05, 2022. [Online]. Available: https://cosmos.network/

[25] A. Fallis, "Rootstock platform: Bitcoin powered smart contracts—white paper," *Journal of Chemical Information and Modeling*, vol. 53, pp. 1689–1699, 2013.

[26] Blockstream liquid network. Accessed Jan. 04, 2023. [Online]. Available: https://blockstream.com/liquid/

[27] Elements — elementsproject.org. Accessed Dec. 05, 2022. [Online]. Available: https://elementsproject.org/

[28] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timón, and P. Wuille, "Enabling blockchain innovations with pegged sidechains," *URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains*, vol. 72, pp. 201–224, 2014.

[29] Loom network – production-ready, multichain interop platform for serious dapp developers. Accessed Dec. 05, 2022. [Online]. Available: https://loomx.io/

[30] Poa merger & swap notice - poa. Accessed Dec. 05, 2022. [Online]. Available: https://www.poa.network/

[31] M. A. Talib, S. Abbas, Q. Nasir, F. Dakalbab, T. Mokhamed, K. Hassan, and K. Senjab, "Interoperability among heterogeneous blockchains: A systematic literature review," *Trust Models for Next-Generation Blockchain Ecosystems*, pp. 135–166, 2021.

[32] W. Li, A. Sforzin, S. Fedorov, and G. O. Karame, "Towards scalable and private industrial blockchains," in *Proceedings of the ACM workshop on blockchain, cryptocurrencies and contracts*, 2017, pp. 9–14.

[33] P. Bennink, L. Gijtenbeek, O. Deventer, and M. Everts, "An analysis of atomic swaps on and between ethereum blockchains using smart contracts," Technical report, Tech. Rep., 2018.

[34] P. Robinson, R. Ramesh, and S. Johnson, "Atomic crosschain transactions for ethereum private sidechains," *Blockchain: Research and Applications*, vol. 3, no. 1, p. 100030, 2022.

[35] M. Herlihy, "Atomic cross-chain swaps," in *Proceedings of the 2018 ACM symposium on principles of distributed computing*, 2018, pp. 245–254.

[36] Home - blocknet documentation. Accessed Dec. 05, 2022. [Online]. Available: https://docs.blocknet.org/

[37] Introduction - wanchain. Accessed Dec. 05, 2022. [Online]. Available: https://docs.wanchain.org/get-started/introduction

[38] What is aion blockchain? the most comprehensive guide ever. Accessed Dec. 05, 2022. [Online]. Available: https://www.blockchain-council.org/blockchain/aion-blockchain/

[39] Ark.io — a blockchain ecosystem built for everyone. Accessed Dec. 05, 2022. [Online]. Available: https://ark.io/

[40] H. Wang, Y. Cen, and X. Li, “Blockchain router: A cross-chain communication protocol,” in *Proceedings of the 6th international conference on informatics, environment, energy and applications*, 2017, pp. 94–97.

[41] ZhongAnTech. (2017) Anlink blockchain network whitepaper v1.0. [Online]. Available: https://alicliimg.clewm.net/049/389/1389049/1484820492640c2baf37ea3e4f9fd77bd52c2a1e9bbbe1484820484.pdf

[42] B. Pillai, K. Biswas, Z. Hóu, and V. Muthukkumarasamy, “Cross-blockchain technology: integration framework and security assumptions,” *IEEE access*, vol. 10, pp. 41 239–41 259, 2022.

[43] B. Pillai, K. Biswas, and V. Muthukkumarasamy, “Cross-chain interoperability among blockchain-based systems using transactions,” *The Knowledge Engineering Review*, vol. 35, p. e23, 2020.

[44] G. Wang and M. Nixon, “Intertrust: Towards an efficient blockchain interoperability architecture with trusted services,” in *2021 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2021, pp. 150–159.

[45] Home — ethereum.org. Accessed Jan. 12, 2023. [Online]. Available: https://ethereum.org/en/

[46] Truffle — overview - truffle suite. Accessed Jan. 12, 2023. [Online]. Available: https://trufflesuite.com/docs/truffle/

[47] Ganache — overview - truffle suite. Accessed Jan. 12, 2023. [Online]. Available: https://trufflesuite.com/docs/ganache/

[48] 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/

[49] Hyperledger caliper. Accessed Jan. 30, 2023. [Online]. Available: https://www.hyperledger.org/projects/caliper

[50] Hyperledger cacti. Accessed Feb. 25, 2023. [Online]. Available: https://www.hyperledger.org/projects/cacti

FAIZA HASHIM received her PhD degree in informatics and computing from United Arab Emirates University, UAE in 2023 and MPhil and Master’s degree in Computer Science from University of Peshawar, Pakistan in 2016 and 2008, respectively. From 2019 to 2023, she worked as a senior researcher at the College of Information Technology, UAEU. Currently, she is pursuing her career as a visiting faculty at United Arab Emirates University and a research consultant at Zayed University, Dubai. Her research interest includes smart healthcare blockchain networks, inter-blockchain communication, machine learning algorithms integration to blockchain networks, and machine learning. Dr. Faiza Hashim’s awards and honors include QUWA Research Award in the 4th Forum for Women in Research, 2023, the Award for Publications in the top 1, 5, 10, and 25% Journals, UAEU, 2021, and the UAEU Fellowship in 2018.

KHALED SHUAIB received the B.E. and M.S. degrees in electrical engineering from The City College of New York in 1991 and 1993, respectively, and the Ph.D. degree in electrical engineering/communication networks from the Graduate Center, The City University of New York, in 1999. Since 2002, he has been with the College of Information Technology (CIT), United Arab Emirates University, where he is currently a Professor. He has over 130 refereed publications in journals and conferences and three U.S. patents. His research interests are in the areas of Blockchains, Smart Healthcare Systems, Cybersecurity, and IoT.

EZEDIN BARAKA is currently an Associate Professor and a Dept. Chair at the College of Information Technology, United Arab Emirates University. He received his Ph.D. in Information Technology from George Mason University, Fairfax, VA in 2002, where he was a member of the Laboratory for Information Security Technology (LIST). His current research interests include Access Control, where he published a number of papers addressing delegation of rights using RBAC. Other research areas include Digital Rights Management (DRM), Large-scale security architectures and models, Trust management, Security in UAVs, and Network “Wired & Wireless” and distributed systems security. Dr. Barka has published over 50 Journals and conference papers. Dr. Barka is an IEEE member, member of the IEEE Communications Society and member of the IEEE Communications Information Security Technical Committee (CISTC). He serves on the technical program committees of many international IEEE conferences such as ACSAC, GLOBECOM, ICC, WIMOB, and WCNC. In addition, he has been a reviewer for several international journals and conferences.

FARAG SALLABI received his Ph.D. in Electrical and Computer Engineering from the University of Ottawa, Canada, in 2001 and the B.Sc. and M.Sc. degrees in Electrical and Electronic Engineering from Benghazi University, Benghazi, Libya, in 1987 and 1995, respectively. He is an Associate Professor at the Department of Computer and Network Engineering and the Coordinator of the Ph.D. Program of Informatics and Computing, College of Information Technology, United Arab Emirates University (UAEU). He served as the Principal Investigator (PI) and Co-PI on several research projects funded by the UAEU. His research interests include quality of service provisioning in wired and wireless networks, routing in wireless sensor networks, performance evaluation of wireless sensor networks, network management, modeling and simulation, Internet of Things, and smart healthcare systems. Dr. Sallabi joined the UAEU in September 2002. He also worked at Sigpro Wireless Company in Ottawa, Canada, from August 2001 to August 2002. Dr. Sallabi has published over 70 refereed publications, including journals and conferences. He is an IEEE member and has served on technical program committees of many international IEEE conferences. In addition, he has been a reviewer for several international journals.