Computers, Materials & Continua
DOI:10.32604/cmc.2021.015354
Article

Tech Science Press

Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records

Mueen Uddin[1,*], M. S. Memon[2], Irfana Memon[2], Imtiaz Ali[2], Jamshed Memon[3], Maha Abdelhaq[4] and Raed Alsaqour[5]

[1]Faculty of Science, Universiti Brunei Darusslam, Gadong, BE1410, Negara Brunei Darussalam
[2]CSE Department, QUEST, Nawabshah, Pakistan
[3]School of Computing and Mathematics, Ulster University, Jordanstown Campus, Newtownabbey, BT37 0QB, UK
[4]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 84428, Saudi Arabia
[5]Department of Information Technology, College of Computing and Informatics, Saudi Electronic University, Riyadh, 93499, Saudi Arabia
[*]Corresponding Author: Mueen Uddin. Email: mueenmalik9516@gmail.com
Received: 17 November 2020; Accepted: 15 February 2021

Abstract: Background: Electronic Health Record (EHR) systems are used as an efficient and effective technique for sharing patient's health records among different hospitals and various other key stakeholders of the healthcare industry to achieve better diagnosis and treatment of patients globally. However, the existing EHR systems mostly lack in providing appropriate security, entrusted access control and handling privacy and secrecy issues and challenges in current hospital infrastructures. Objective: To solve this delicate problem, we propose a Blockchain-enabled Hyperledger Fabric Architecture for different EHR systems. Methodology: In our EHR blockchain system, Peer nodes from various organizations (stakeholders) create a ledger network, where channels are created to enable secure and private communication between different stakeholders on the ledger network. Individual patients and other stakeholders are identified and registered on the network by unique digital certificates issued by membership service provider (MSP) component of the fabric architecture. Results: We created and implemented different Chaincodes to handle the business logic for executing separate EHR transactions on the network. The proposed fabric architecture provides a secure, transparent and immutable mechanism to store, share and exchange EHRs in a peer-to-peer network of different healthcare stakeholders. It ensures interoperability, scalability and availability in adapting the existing EHRs for strengthening and providing an effective and secure method to integrate and manage patient records among medical institutions in the healthcare ecosystem.

Keywords: Electronic health records; blockchain; hyperledger fabric; patient data privacy; private permissioned blockchain; healthcare ecosystem

1 Introduction

Electronic Health Record (EHR) is a health-related critical and highly sensitive information for the diagnosis and treatment of patients under care [1,2]. There is a continuous and dramatic increase in the volume of patient's data through multiple EHRs as existing EHRs have limited scope and accessibility because of scattered data as it belongs to specific patients and hospitals. One of the most significant and severe challenges the healthcare industry currently facing is the access, sharing, and rational distribution of EHRs among innumerable healthcare stakeholders such as hospitals, doctors, pharmacies, labs, insurance companies, researchers, and patient families. For instance, a patient with HIV or cancer disease has to keep and maintain a long history of treatment plan, medical diagnostic tests and reports, and post-treatment rehabilitation and monitoring process. Providing access to this information, storing, sharing, and distributing it among multiple healthcare stakeholders is crucial for keeping the patient's medical history up-to-date, proper laboratory tests and diagnosis, treatment, and wellbeing of the patient [3]. It gives rise to several vulnerabilities and challenges, including tampering, stolen, deletion, privacy, secrecy, and interoperability of this personal healthcare information resulting in delayed and erroneous treatment that ultimately endangers patient's life [4–7].

The EHRs are usually stored in the repositories of healthcare service providers and are often not shared between service providers or even with patients. On the contrary, when these medical records are shared, there are barriers to achieving it [8,9]. For example, interoperability stemming from various healthcare platforms and data standards can lead to both administrative and clinical errors [10]. Furthermore, the integration of large volumes of medical data causes inefficiencies and tiresome while recounting and re-informing the history of patients, repeated laboratory tests and their results, as well as different prescriptions of pharmaceutical drugs and unnecessary tests. It leads to severe confusion and clinical errors because of duplicated and incomplete information from various stakeholders [11].

So far, countries like the U.S, Canada, and the European Union have already started several projects to build redesign and upgrade existing EHR systems to integrate patient's health records and medical histories. One of the most significant healthcare projects run and managed by CommonWell Health Alliance in the U.S. [12] provides a nationwide interoperability mechanism to connect and share existing EHRs, hospitals and healthcare information technology (HIT) systems and networks via certified integration platforms and intermediaries. However, this system is complicated, slow, difficult to achieve scalability, security, and privacy among patients EHRs leading to situations where lack of security and privacy measures and information shortage can cause severe clinical repercussions [13]. The centralized architecture also poses a grave threat and risk of single-point-of-failure and efficiency issues such as bottleneck of patient's data flow when its volume increases in size and quantity. These existing EHR systems also need to keep and protect the log files used for recreating the previous state of medical records and histories of patient's data, and this file is a legal document. It must be protected against all types of vulnerabilities.

In this paper, we reflect on the potential of blockchain technology for providing a decentralized, secure, and trustable EHR system using a private permissioned blockchain architecture to address the problems and challenges in sharing and exchanging patient records among the existing EHRs systems. The proposed Hyperledger Fabric architecture is immensely compliant and acquiescent with the Health Insurance Portability and Accountability Act (HIPAA) and ISO/TS 18308 [14]. It enables us to create a shared, immutable, secure, scalable, and interoperable architectural solution that empowers patients and hospitals with more transparency, privacy

and security while collecting and retrieving sensitive patient data from various integrated, connected but independently managed EHR systems. The significant contributions of our work are as follows:

- We review and highlight the reasons as to why the existing EHRs needs a private permissioned blockchain-enabled EHR solution.
- We present Hyperledger Fabric blockchain architectures for EHRs to create a trusted and transparent encyclopedia of patient data in EHRs that pledges controlled data access and integrity among the stakeholders of the EHR system.
- We present how our proposed hyperledger fabric architecture strengthens the privacy and secrecy of patient data by incorporating more enhanced encryption methods to provide an undeniable audit trail based on an immutable access log compared to existing solutions.
- We present a complete sequence flow of all medical transaction record activities among the stakeholders to illustrate a completely scalable and interoperable solution among the existing EHRs of regional or core hospitals without relying on a centralized controlled and management system.
- We identify, enumerate, and discuss several future research challenges that may hinder the successful deployment of blockchain solutions in the drug supply chain.

The rest of this paper is organized as follows; in the next section we present problem background highlighting existing solutions in EHR. In section 3 we present and discuss the proposed blockchain enabled hyperledger fabric architecture for the efficient and secure management of EHRs, in section 4, we discuss the implementation of proposed solution through sequence diagrams between various stakeholders in the healthcare ecosystem. In section 5, several limitations and open challenges pertaining to adoption of blockchain technology are addressed. In section 6, we present the conclusions and future work.

2 Problem Background and Existing Solutions

The current EHR management systems provide a tedious way to keep track of the chronological progression of the patient's current health status [15]. These existing systems have left an incompletely digitized complex where paper records remain ubiquitous at various levels in hospitals, labs, and pharmacies with disconnected trustless electronic systems leading to the administrative problems of security, integrity, scalability, and interoperability [16]. The healthcare industry has been a significant target of cybercrime-related attacks where patient-related information (EHR) such as names, social security numbers, and addresses are being theft and modifies, instigating data integrity, privacy, and confidentiality related problems in the existing EHR systems. In the year 2015, around 79 million patients' records were hacked and stolen from the servers of the Anthem insurance corporation [17]. In the year 2017, the attacks on the U.S. Department of Health affected around 2.6 million patient's data [18]. Furthermore, in the year 2017, WannaCry, a global ransomware cybercrime attack, directly affected, and crippled 80 of the total 236 National Health Service (NHS) trusts [19]. It also affected FedEx and more than 300000 server machines were infected in over 150 countries around the world and is considered as the "the biggest ransomware outbreak in history" [20].

Recently, the theft of EHRs is rapidly becoming ubiquitous as a result of feeble security measures, systems, and policy enforcement as the records are stored in standard databases controlled and maintained by service providers. A blockchain-enabled EHRs management system provides transparency, interoperability, security, and creates trust amongst the healthcare stakeholders by replacing the third-party service providers [21]. It enables us to trace and track all the

patient-related activities and events by providing individual details of patient-related transactions such as (medical history, tests, diagnosis, medicines, and post medical care) and stores it in an immutable and shared ledger [22]. Tab. 1 provides a summary of healthcare data management mechanisms in blockchain technology.

Table 1: Comparison of the medical record management for healthcare in blockchain technology

Blockchain technology	Type of medical data	Merits	Demerits	Article
Private Blockchain (Proof-of-Ownership)	EHR	Secure sharing of healthcare-related data and improved auditing process	The scope is limited to Europe for cross-border exchange of E-health data.	[23]
Private blockchain	EHR & PHR	AI-based blockchain solution for privacy control in sharing healthcare data	The proposed solution was not scalable, and the availability of data was also not guaranteed (sharing of E-health data is limited).	[24]
Proof-of-Stake	Medical image records	Secure and decentralized sharing of medical imaging data	The proposed solution doesn't consider privacy and interoperability issues	[25]
Hybrid consensus mechanism based on practical byzantine fault tolerance	EMR	Secure medical data sharing using block enabled blockchain solution	Medblock failed to consider privacy and confidentiality issues related to the patient's identity	[26]
Proof-of-work	Telecare medical information system	Medical data is shared based on Multi-layer location sharing schema	Solution lacks the justification and critical condition under which a patient's location data was retrieved and repossessed	[27]
Private Blockchain	EHR	Secure sharing of E-health data among healthcare stakeholders	Solution lacks in providing a mechanism for handling high storage data, and breadcrumb process is looking up for single record each time	[28]

(Continued.)

Table 1: Continued

Blockchain technology	Type of medical data	Merits	Demerits	Article
Ethereum platform	EMR	EMR management and sharing of medical data using cloud	The solution failed to provide essential replacement capability and privacy	[29]
Hyperledger platform	EMR	consent management in managing and sharing personal data in E-health systems	Access control and exhaustive authorization process are completely missing	[30]
Consortium blockchain	Medical records	Medical record sharing using coupled encryption and signature-based robust security	The proposed solution is not fully functional and automated	[31]
Ethereum platform	Healthcare data	Cost-effective smart contracts for sharing and storing healthcare data	Interoperability and scalability are not considered as part of the solution between stakeholders	[32]
Hyperledger Fabric blockchain	EMR	MedBloc: Blockchain-based secure EHR system for sharing and accessing medical data	This system didn't consider privacy and confidentiality challenges pertaining to patient's identity	[33]
Hyperledger Fabric blockchain	EHR	Identity and access management with blockchain technology in EHRs	The EHR system failed to provide secure and scalability solution	[34]
Block based Access control system from an EMR Server using IoT	EMR	Block-based access control for blockchain-based EMRs query in eHealth	The scope was limited to only single hardware enabled IoT server of various EMR data	[35]
Public Blockchain (Ethereum)	EHR	Secure, interoperable and scalable sharing of clinical data	The solution failed to provide shared decision-making mechanism	[36]
Public blockchain	EMR and PHR	Blochie: A blockchain-based platform for recording and storing healthcare data	Scalability and interoperability are not considered as main factors while developing the solution	[37]

(Continued.)

Table 1: Continued

Blockchain technology	Type of medical data	Merits	Demerits	Article
Proof-of-interoperability	EHR	Sharing of healthcare information for clinical and research purposes	It lacks in providing access control and privacy features while sharing medical data	[38]
Consensus blockchain	Image archiving and communication systems	Exchange of medical images	Fail to handle access control, privacy and interoperability challenges	[39]
Consortium blockchain	PHR	Sharing of health data between health enterprises for usage	The proposed solution doesn't consider Access control and data interoperability features	[40]
Secure attribute-based blockchain (public blockchain)	EHR	Sharing of health data between health enterprises for usage	Data Integrity and privacy of patient's data is not considered while sharing health data	[41–43]
Hash enabled blockchain platform	EHR	Sharing of health records for clinical, administrative and research purposes	Access control & confidentiality are not considered	[44]
PKI enabled blockchain	EHR	Retrieving, storing and exchanging healthcare-related information in EHR	The proposed solution is not designed to cater to access control, privacy and data integrity	[45]

3 Current EHR Challenges

The transition of blockchain technology from hype to reality poses serious challenges, especially in the context of the healthcare industry, where the storage, transfer, and interoperability of EHR are the significant concerns that need to be solved using blockchain-enabled solutions. To ensure the better utilization and implementation of blockchain, it requires a good understanding of the technology as well as what it entails to achieve the desired objectives. Some of the challenges that current hyperledger forum and business organizations facing described below:

Data privacy: A blockchain network is a distributed ledger where all healthcare stakeholders, including patients, store their core electronic medical data, and everyone has access to this sensitive private data on the platform. It creates serious privacy challenges as the majority of patients, and other stakeholders do not want to leverage their private data against their competitors. Subsequently, many potential stakeholders feel shy and reluctant to participate in the network for fear of losing their competitive advantage, especially when other organizations are business rivals in the supply chain such as insurance companies and pharmacies.

Data and enterprise platform interoperability: Interoperability is defined as a mass adaption of business software and platforms across multiple organizations to provide effective and efficient services to the end-users as well as users of different platforms and software to interact and conduct meaningful businesses. The existing EHR solutions, as well as blockchain-enabled solutions and platforms, lack interoperability solutions as there is a disconnection among these implementation platforms, which makes adaptability and implementation difficult. Recently different blockchain platforms under the umbrella of hyperledger are trying to cope up with this issue to provide interoperability solutions to ensure maximum scalability and adaptability for enabling inter-communication among different healthcare organizations.

Security: One of the most significant advantages and selling points of blockchain technology is its resilience against various types of attacks, including cyberattacks. A recent cybersecurity report highlights several security risks, including bad actors involved in the blockchain network and exposing the implementation network to the hackers. The current blockchain implementations are leaving inherent vulnerabilities and bugs due to the development of immature processes and systems. For instance, phishing scams, technology vulnerabilities, implementation exploits, and malware due to the unavailability of standards and procedures are causing severe challenges.

Lack of Standardized Regulations: The role of health regulatory authorities includes checking and maintaining the quality, safety, efficacy, transfer, and exchange of EHR among various healthcare stakeholders. These health authorities oversee the retrieval, storage, transfer, and exchange of EHR data in a more secure, transparent, scalable, and interoperable way so that patient's health-related issues and challenges can be dealt with in a more efficient and well-organized way to provide better health solutions. In blockchain-enabled solutions, the role of regulatory agencies become more pertinent and complicated as it becomes hard for these health authorities to define the legal boundaries and environment for blockchain technology. For instance, when a new patient transaction is executed on the network, it is difficult for these authorities to clearly define the jurisdiction and correct legal obligations for the stakeholders involved. Another challenge is to cope with the requirements of upcoming legislations such as DSCSA, FDA, CFDA, and GDPR, in blockchain networks. Therefore, blockchain technology is still not precise on recent laws and regulations regarding the existing healthcare systems.

4 Private Permissioned Blockchain-Enabled EHR Management

The recent advancement and evolution in EHRs data, IoT enabled EHRs data sharing and storage systems, and healthcare regulations pertaining patient's data privacy, confidentiality and secrecy are creating new opportunities and challenges for the efficient management of EHRs data. Blockchain technology has immense potential to cater to these critical issues robustly and effectively. Blockchain is an encryption enabled system that provides decentralized and distributed ledger for storing, transferring, and viewing secure peer-to-peer (P2P) healthcare-related transactions across mutually untrusted network stakeholders [46]. According to IBM, 75% of healthcare leaders envisage that the most significant impact of blockchain in the health domain will be the improvement of efficient management of storing and sharing of different types of EHRs, clinical trial management, and drug traceability and provenance solutions [47].

Blockchain ensures that the majority of the network nodes must validate the information blocks stored on the ledger before being posted to the ledger based on stated and agreed rules. One of the strengths of blockchain is that the stored blocks are immutable, reliable, secure, and trusted as they require verification and validation from the majority of the network nodes and have no single point of failure. It enables us to create trust between various healthcare entities,

stores immutable records, provides consensus mechanisms, uses private keys, and decentralized networks to enable secure and transparent communication between untrusted parties in the EHR data management system. A private permissioned blockchain is suitable in achieving patient's privacy and confidentiality, such as their healthcare-related private details. It focuses on specific security and interoperability vulnerabilities and challenges and solves the barriers of existing EHR systems described in the above section. It bridges the gap between the existing EHR systems and enables us to create an immutable, auditable, scalable, and interoperable systems for efficient management of EHRs in the healthcare industry. Blockchain-enabled efficient EHRs system showing the secure workflow of patient records and activities are illustrated and explained in Fig. 1. It comprises of seven (7) steps mentioned below:

Step-1: Initially, the patient visits the physician (doctor) by registering itself to the hospital counter. This patient data consists of medical history, current problem and other physiological information and is stored in the local database connected to the system.

Step-2: An EHR is generated from the initial data collected in step (1) for each patient. Additionally, other medical information such as laboratory test results, medical imaging, nursing care, and drug history-related data will also encompass the EHR.

Step-3: The patient who is the owner of EHR has the sole authority to give different access rights and permissions of sharing and using the sensitive information to various stakeholders of the healthcare ecosystems to achieve data privacy and secrecy.

Step-(4–6): The EHRs have now been stored permanently in the blockchain ledger and other decentralized storage systems. The local database is used to make sure that patient records at initial stage can be modified and stored locally before being updated at the ledger.

Step-7: Hospitals and *ad hoc* clinics, are one of the critical stakeholders who have authorized access to the blockchain ledger to provide better and efficient medical services to the patient using the EHRs. This blockchain-enabled EHR system ensures the secure and transparent transfer of EHRs to various healthcare providers in the globe so that the patient's records can be made available and accessible any time at any place validated and verified through a distributed ledger.

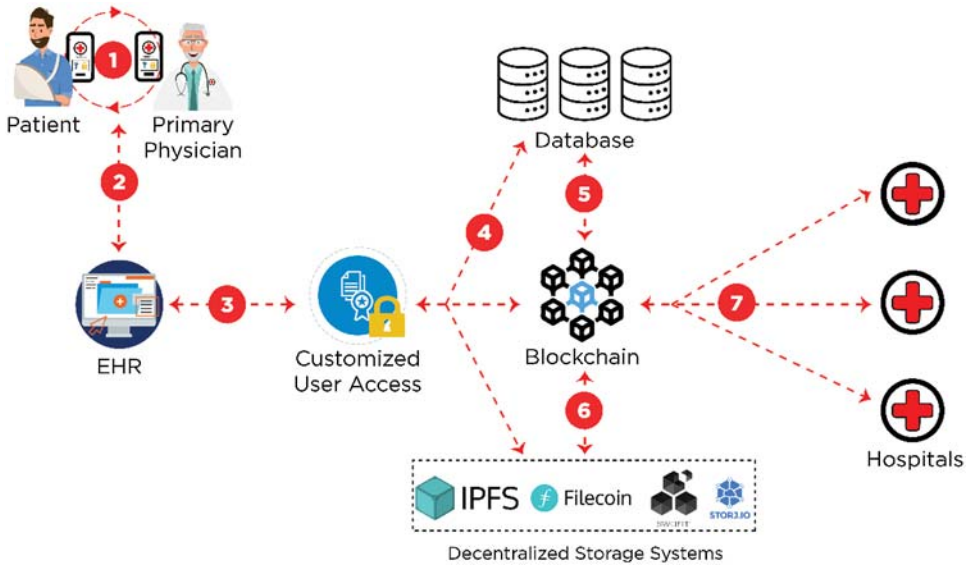

Figure 1: Blockchain-enabled EHRs management in healthcare

4.1 Proposed Hyperledger Fabric Enabled Blockchain Architecture for EHRs

In this section, we describe the development and working principles of our proposed hyperledger fabric architecture for efficient healthcare data management such as storage and transfer of EHRs between healthcare service providers to attain better treatment for patients. We choose Hyperledger Fabric as it provides privacy, scalability, transaction efficiency, interoperability, and fine-grained access control over EHR data and significantly reduces the turnaround time for EHR storage and sharing, improves decision making for medical care, and reduce the overall cost. The proposed fabric architecture enables us to create private permissioned blockchains where different healthcare stakeholders and their end-users are identified, registered, and connected using different channels to provide maximum privacy, confidentiality, data secrecy, and scalability. It provides a secure and transparent Byzantine-fault tolerant (BFT) consensus algorithms for ensuring secure and reliable communication and exchange of health-related data amongst the group of untrusted stakeholders [48].

We choose Hyperledger enabled private permissioned consortium blockchain, which uses the Hyperledger Fabric platform. In the proposed architecture, multiple hospitals are connected to form a private peer-to-peer consortium network. The permission to join the fabric network is determined based on consensus among the participating stakeholders. The fabric uses the Byzantine fault-tolerant consensus protocol for ordering and execution of transactions to the ledger. Furthermore, the efficiency of fabric is much more compare to other public blockchains as it executes more than 3,500 transactions per second. Some of the unique features of fabric relative to other distributed ledger technologies are:

- It provides a private permissioned and modular architecture for executing different transactions in peer-to-peer blockchain network.
- The flexible, pluggable endorsement model helps in realizing and attaining consensus among the stakeholders in the network.
- It provides a mechanism that supports transaction privacy and integrity by using channels. It enables us to create channels among separate member organizations to communicate to accomplish the notion of privacy and secrecy.
- It provides appropriate governance and versioning of chaincodes.
- The transaction processing has less latency compared to other blockchain platforms.
- The smart contracts can be written in multiple languages such as Go, Java, JavaScript.
- It supports different types of queries such as keyed queries, range queries, and JSON on-chain queries.
- It provisions continuous organizational operations, such as rolling upgrades and asymmetric version support.

4.2 Working of Hyperledger Fabric

In the fabric architecture, a permissioned private blockchain network is created where all the participating healthcare stakeholders and their end-users are identified and registered by the health authority using the membership service (MSP) component of the fabric using certificate issuing (C.A.) authorities. These C.A.s can be fabric-based (local) or external to the participating organizations in the blockchain network. To create a trusted environment between untrusted participants, the fabric provisions an identity management system that introduces the notion of membership service that established rules and regulations by which different stakeholders (identities) are governed, authenticated, validated, and verified to be part of the network and allowed to access the EHRs systems for ensuring secrecy, privacy, and confidentiality among the

stakeholders in the network. The membership service is a new comprehensive novel design that revamps the whole process of nondeterminism, resource exhaustion, and performance attacks in the participating stakeholders in health record management systems [49]. The fabric network comprises different peer nodes, and each peer node can be an endorser or committer node. It also contains an ordering service component, also called Orderers. This service accepts the endorsed transactions from the client (patient), orders them into groups of blocks with cryptographic signatures of the ordering peers, and finally broadcasts these blocks to the committing peers in the blockchain network for validations against the endorsement policies as shown in Fig. 2.

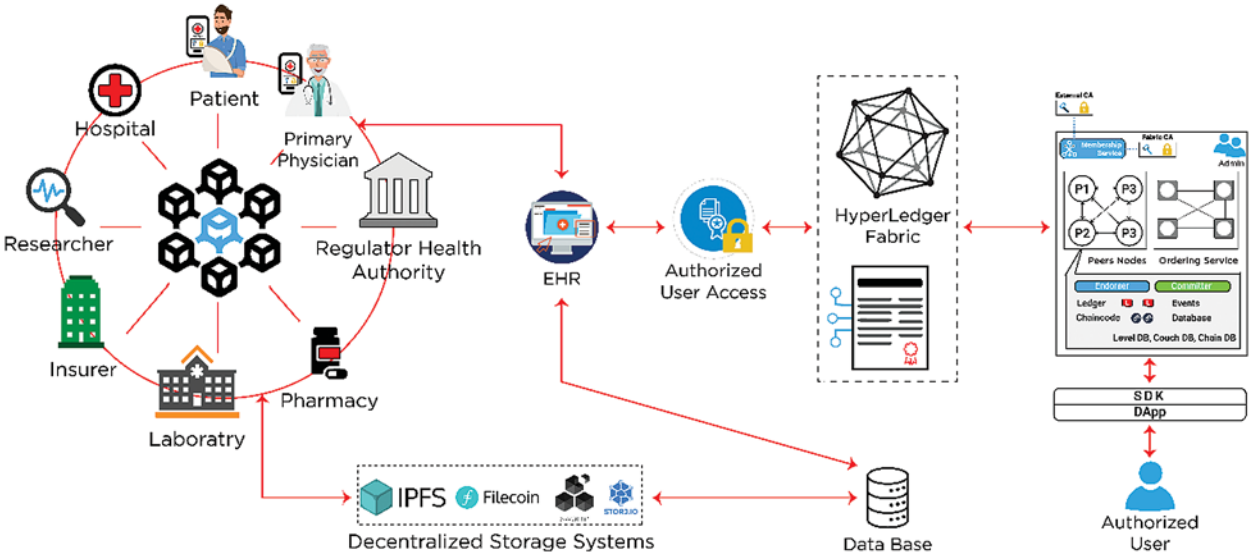

Figure 2: Hyperledger fabric blockchain architecture for EHRs

5 Implementation of Proposed EHR Architecture

In this section, we describe how electronic health record-related transactions are executed and communicated between different stakeholders using execute-order-validate architecture in the fabric. The proposed fabric enabled EHRs system perpetually records and stores all transaction-related activities and events involving all the participating stakeholders in the blockchain's immutable ledger linked with a peer-to-peer decentralized storage system for providing maximum transparency and storage facility to store extensive medical records. The fabric-based decentralized EHRs system significantly diminishes the likelihood of meddling with stored data in the ledger. Additionally, all participating entities are required to identify and authenticate themselves using digital certificates and cryptographic functions through MSP service. Initially, all the participating stakeholders in the healthcare ecosystems are identified and registered by the healthcare authority in peer-to-peer blockchain network.

A registration function will be executed in the smart contracts (chaincode) to register the stakeholders by the designated private regulator health authority that manages and controls the fabric network. It creates a private permissioned network, visible only to the stakeholders registered with the healthcare authority. All stakeholders will be running an extra layer of security by connecting to the registration system through a virtual private network (VPN). While Registering,

patient will only provide the registration **(Add(Patient Record))** information, e.g., Name, SSN, Address, Contact etc. Similarly, the primary physician, hospital, laboratory, pharmacy, researcher and insurer will also register with the regulator healthcare authority, as shown in Fig. 3. above. Once registered, the health authority will verify the record **(Verify(Patient Record))** and assigns a chaincode address **(Create(Patient Address))**. This procedure completes the registration process, and all the stakeholders are ready to perform the transactions on the network.

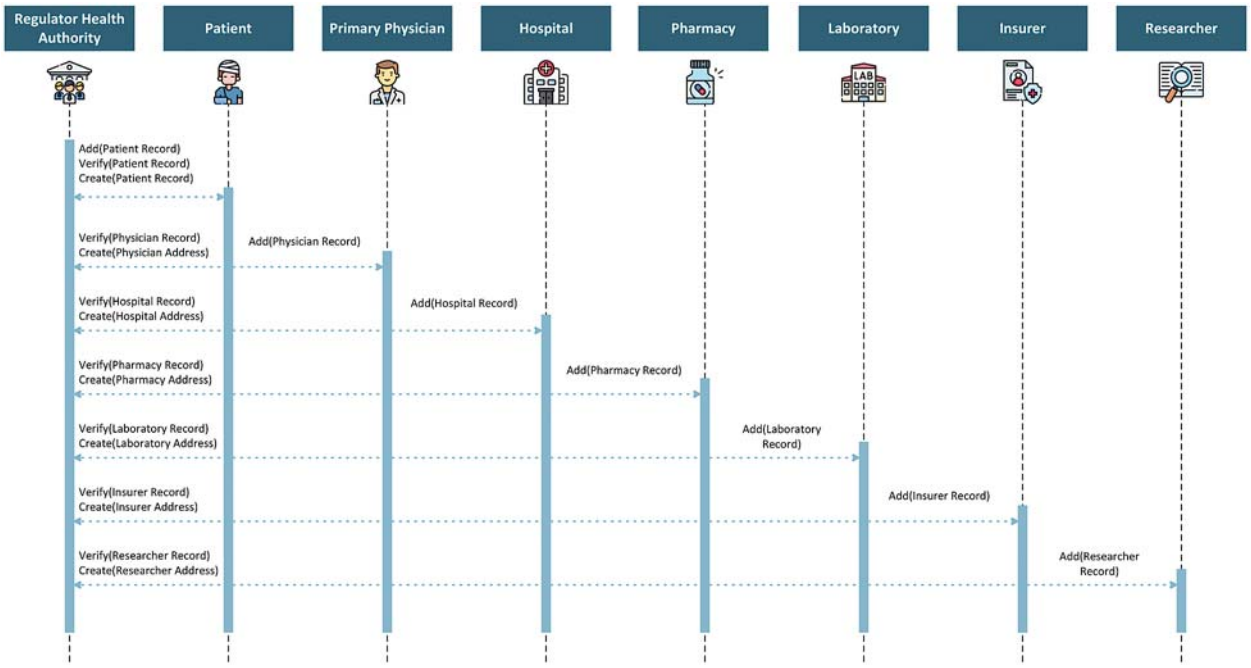

Figure 3: Stakeholder registration in EHRs healthcare ecosystem

5.1 Transaction Flow in Hyperledger Fabric EHR Architecture

In the proposed fabric architecture, initially, the patient proposes a transaction or transaction proposal (execute a specific function on the chaincode). The transaction proposal request will be submitted to the peer nodes (endorsers) as determined by the endorsement policy in the fabric. The EHR proposal consists of different parameters such as patient identification information according to the membership service provider, the transaction payload that includes the list of operations to be performed, the chaincode identifier, a nonce value (counter or random value) to be used only once by the submitting user and transaction proposal identifier as given in algorithm below. The algorithm describes a chaincode where different transaction activities performed by the patient are shown in the form of different functions. This phase is called the endorsement phase or the proposal phase.

Algorithms: Chaincode of various patient's activities in proposed EHR system

```
Chaincode 1: Patient Hospital Appointment
@HospitalAppointment( )
    Public AppointmentRequest(String PatientID, String PhysicianID, String HealthRecord)
    If Slotavaiable(DateAndTime)
    GrantAppointment(String PatientID, String PhysicianID, String HealthRecord, Time
    DateandTime)
Return DateandTime

Chaincode 2: Patient Check-up and Treatment
@CheckupAndTreatment( )
  Public Checkup(String PatientID, String HospitalID, String PhysicianID, String HealthRecord)
Return PhysicianRecommendations
  If PhysicianRecommendations contains LabTests
      ConductLabTests(String Patient, String Hospital, String HealthRecord, String TestType)
      Return LabTestReport
  If PhysicianRecommendations contains MedicalProcedure
      ConductMedicalProcedure(String Patient, String Hospital, String HealthRecord, String
      Procedure)
      AdmitPatient(String Patient, String Hospital, String HealthRecord, String Room/Ward)
      ConductProcedure(String Patient, String Hospital, String HealthRecord, String Procedure,
      Status)
      CollectMedicine(String Patient, String Hospital, String HealthRecord, String Prescription)
      PatientDischarge(String Patient, String Hospital, String HealthRecord, String
      DischargeNote)

Chaincode 3: Payment
@Payment( )
  If PatientID.PaymentType contains Selfpaying
     SelfPayingPatient(String Patient, String Physician, String HealthRecord, String Cost)
  Else if PatientID.PaymentType contains Insurance
     ClaimgInsurance(String Patient, String Physician, String HealthRecord, String
     InsuranceCost)

Chaincode 4: Medical Record Update
@MedicalRecordUpdate( )
    PatientUpdate(String Patient, String Physician, String HealthRecord, String Condition)
    PhysicianDecision(String Patient, String Physician, String HealthRecord, String
    PhysicianNote, Decision)
```

The patient transaction proposal will be simulated and executed by a specific number of endorsement peers, as listed in the endorsement policy. The patient transaction proposal has to satisfy the defined endorsement policy for that particular chaincode. This endorsement policy specifies the set of peers on a given channel that must endorse or approve the given transaction proposal. These peers must execute the chaincode and endorse the results acheived after the execution of chaincode functions in order to validate the proposed transaction proposal. The execution results in the form of output will be encrypted and recorded along with the cryptographic signatures of the endorsement peers, and the resulting message is called an endorsement.

This endorsement consists of R.W. (*readset* and *writeset)* values along with other useful information called metadata that includes transaction I.D., endorser I.D., and endorser signature. This endorsement will be sent back to the patient as a response to the transaction proposal submitted. It is essential to highlight that; the patient node will continue to collect all the endorsements until it satisfies the endorsement policy, and until this time, the transaction will not be committed to the ledger. After the proposal endorsement phase, the patient, after receiving enough responses from the endorsing nodes, assembles all the endorsements and broadcasts them to the ordering-service (O-S) in the fabric. The transaction response consists of transaction payload, transaction metadata, and set of endorsements. The ordering service uses pluggable consensus protocols to calculate and establish the execution order of all the submitted transactions in sequence per channel [50]. Furthermore, multiple similar EHR transactions are consigned into blocks (hash chained sequence of blocks) containing submitted endorsed transactions by the ordering service. The consignment process into blocks helps to improve the overall throughput of the broadcast protocols in the transaction flow cycle in the fabric. This phase is called the execution phase. The ordering service then collects all the transactions combined with state dependencies in groups for distribution purposes and broadcasts them to the committing peers in the fabric network, as shown in Fig. 4.

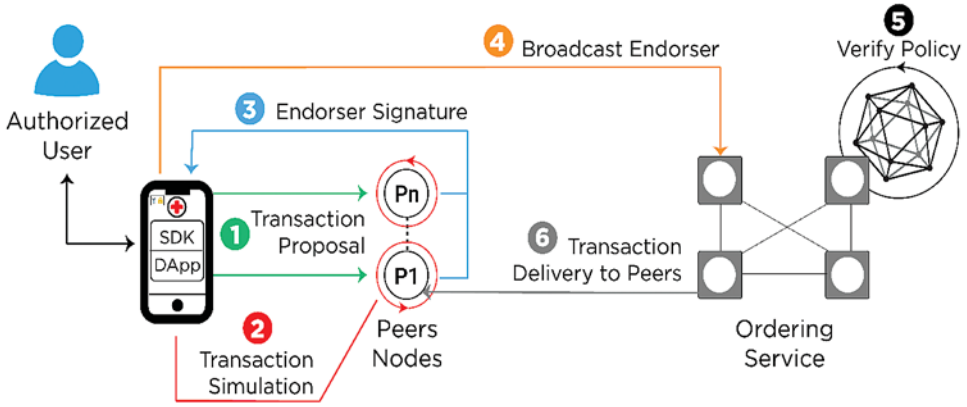

Figure 4: Implementation of transactions in fabric architecture

5.2 Sequence Diagrams

In this section, we describe a secure and efficient working procedure in which a patient's registration information will be recorded on the blockchain ledger. In the first step, when a patient visits a hospital for a checkup, the patient registration process is initiated at the registration desk, and the patient's registration information is recorded in the local EHR database if it's not already available in the database.

This information is encrypted using an appropriate encryption technique with a symmetric key. This private symmetric key is then further encrypted using patient's public key and attached with the patient's encrypted data. This process not only secures the key and data but also fastens the encryption-decryption process while patient data is stored on the ledger. Furthermore, this encrypted information is appended to the ledger in the next step, as shown in Fig. 5 below.

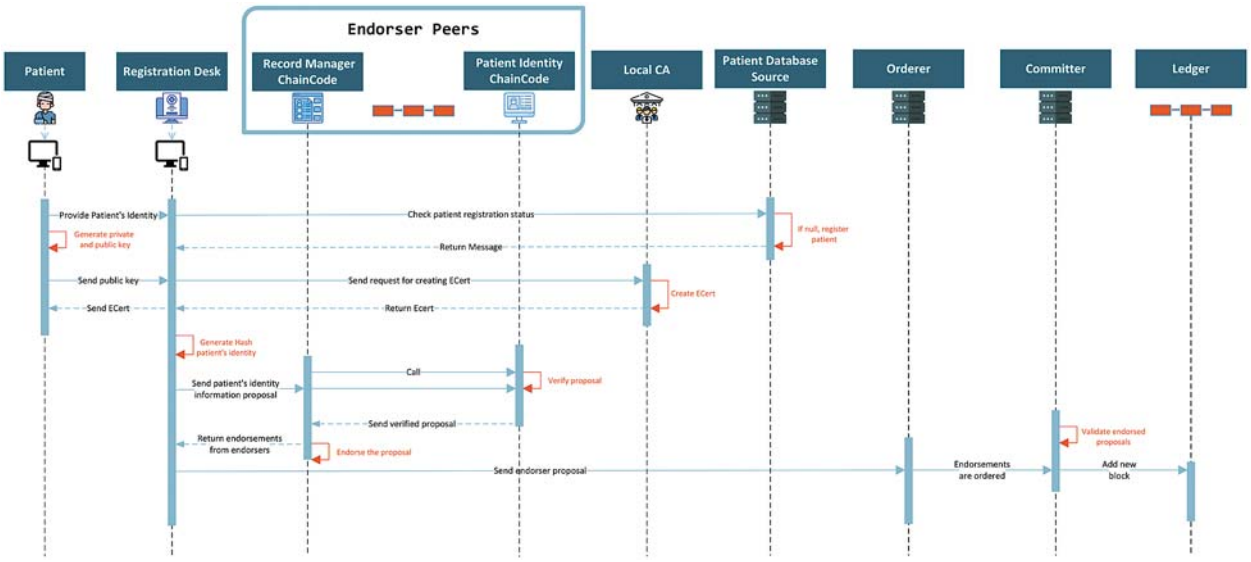

Figure 5: Sequence diagram for patient registration

In the next step, we describe the transaction flow when a patient visits the primary physician. In this phase, the primary physician sends a transaction proposal to get the patient-related previous metadata information (if any) if patient has already visited the physician from the ledger in the hospital. The patient information is returned to the physician if it's available in the ledger; otherwise, the patient will be considered as new patient and physician will do the checkups and sends the updated patient information to the ledger after checking the patient. This process is shown in Fig. 6 below. Where patient records are updated and appended in the ledger after visiting physician and the same information will be shared to the patient and other stakeholders participating in the fabric network. The patient visits the primary physician **(AppointmentGranted(Patient, Physician, HealthRecord, Date & Time))** after requesting an appointment **(AppointmentRequest(Patient, Physician, HealthRecord))**. Fig. 6 illustrates a sequence diagram where transaction between patient and primary physician, which later involves all other stakeholders are shown in the hyperledger fabric. After the initial consultation **(CheckupDone(Patient, Physician, HealthRecord)** the physician refers the patient to the diagnostic laboratory for conducting tests **(LabTestsConducted(Patient, Physician, HealthRecord, LabTests, Results))**.

Based on the results, the physician recommends medicine **(MedicineCollected(Patient, Physician, HealthRecord, Prescribed Medicine))**. The patient pays the bill either via insurer **(InsuranceClaimed(Patient, Physician, HealthRecord, InsuranceCost))** or self in case patient is not insured **(SelfPayingPatient(Patient, Physician, HealthRecord, Cost))**. In countries where healthcare is mostly free, this may never happen. Patient may visit the Physician for follow-up consultation and physician will submit the report about the condition of the patient **(PatientUpdate(Patient, Physician, HealthRecord, Condition))**. Once the patient gets well, all the completed transactions, including physician decision transaction **PhysicianDecision (Patient, Physician, HealthRecord, PhysicianNote, Decision)** will be appended as a block to the fabric hyperledger after a particular transaction is complete and validated by a designated number of peers (endorsers and committers) on the network.

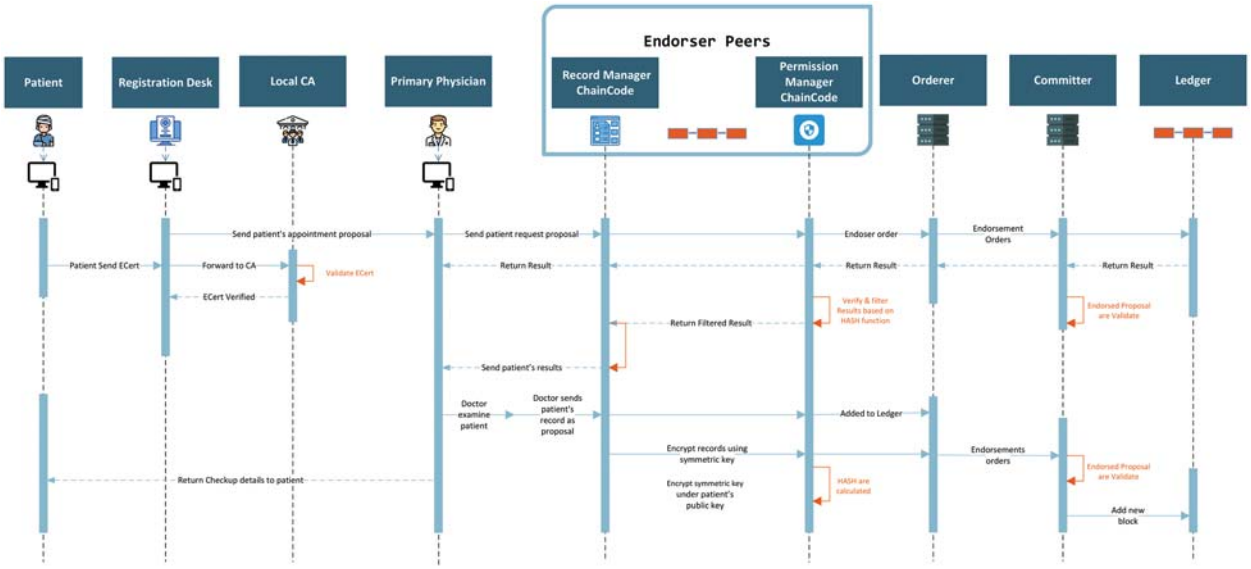

Figure 6: Sequence diagram showing patient checkup process by the physician

Some of the transactions that require more storage will be stored in the decentralized storage, and their hash values will be stored at the ledger. It is essential to highlight that some of the transaction such as patient registration will remain in a temporary database until it is complete and patient no longer need to see the physician for the consultation until the situation arises next time. A Researcher may request for the access to data for research purpose **(RequestToAccessData(Patient, HealthRecord))** and a patient may either grant or deny the access to medical data **(RequestStatus(Patient, AccessGranted/Denied))**. This permission may vary from country to country depending on the privacy and data protection laws. Permission to grant or deny access to EHRs lies with the patient or the health authority.

The functional transactions between the patient and the hospital are described and illustrated in Fig. 7. It is possible that after the initial consultation, the primary physician may refer the patient to the hospital depending on the severity of the condition **(PhysicianRecommendsHospital(Patient, Physician, HealthRecord, Hospital))**. It is also possible that the patient can be directly admitted to the hospital instead of being referred by the physician. In this case, the patient is referred to the hospital by another physician from another hospital. The hospital gives an appointment to the patient and does the initial consultation **(HospitalAppointmentGranted(Patient, HealthRecord, Hospital, Date & Time))(CheckupDone(Patient, Hospital, HealthRecord))**.

Patient will then go through the diagnostic process in which the laboratory tests and their results will play an essential role in determining the root cause of the disease **(LabTestsConducted(Patient, Physician, HealthRecord, LabTests, Results))**. The hospital will perform a surgical or non-invasive procedure after the diagnostics **(MedicalProcedureRecommended(Patient, Hospital, HealthRecord, Procedure))** and may admit the patient into the ward for the recovery **(PatientAdmitted(Patient, Hospital, HealthRecord, Room/Ward))**. The patient will collect the medicines before being discharged **(MedicineCollected(Patient, Hospital, HealthRecord, Prescription))** from the hospital. Payment can either be made via insurer or self **(SelfPayingPatient(Patient, Physician, HealthRecord, Cost)) (InsuranceClaimed(Patient, Physician, HealthRecord, InsuranceCost))**. All

these transactions once complete and validated and verified by appropriate number of peers (endorsements) will then be permanently stored to the hyperledger as shown in Fig. 8.

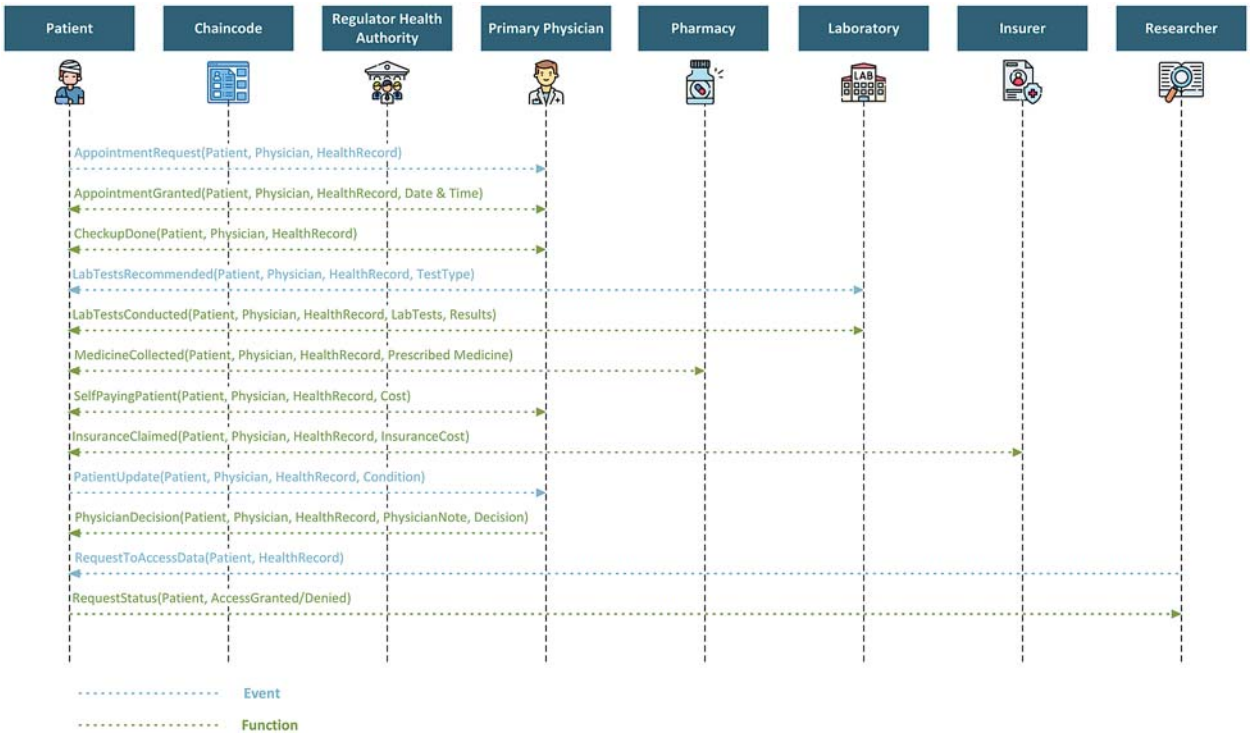

Figure 7: Transaction flow between patient and doctor

6 Hyperledger Fabric Implementation Challenges and Opportunities

To ensure the better exploitation and implementation of blockchain architecture, it necessitates a good understanding of the technology as well as what it entails to achieve the desired objectives. The private permissioned Fabric architecture poses several significant challenges and opportunities for the healthcare industry as it's not a fully matured platform nor a remedy solution to be implemented proximately. It requires us to address different organizational, technical and performance-related challenges before a blockchain-enabled EHRs solution can be implemented and adopted by various organizations worldwide. Some of the problems current hyperledger forum and business organizations facing today are described below:

Scalability Limitations: The global spending on blockchain solutions will reach around $12 billion by 2022, as reported by IDC, pushing for highly demanding and proficient blockchain-enabled solutions for different enterprises. A majority of the existing blockchain platforms are untested and unregulated to provide scalability services at large scale with high success rates. The scalability also restricts the size of the data, transaction processing speed, and latency in data processing capabilities in the blockchain network. In the context of healthcare EHRs, permissioned private blockchain solutions are considered more useful as they provide broader access control mechanism, allow for better innovative solutions and have much higher processing and executing efficiency (35000 transactions per second) as well as higher computing power across the network

compare to permissionless public blockchain solutions [50]. It is, therefore, imperative to highlight that numerous enterprise blockchain projects must undertake assurance for the global market that their platforms are sufficiently scalable for implementing the blockchain solutions at the enterprise level. A comprehensive blockchain solution, with a large number of healthcare stakeholders, would make the EHRs system more interoperable and secure [51].

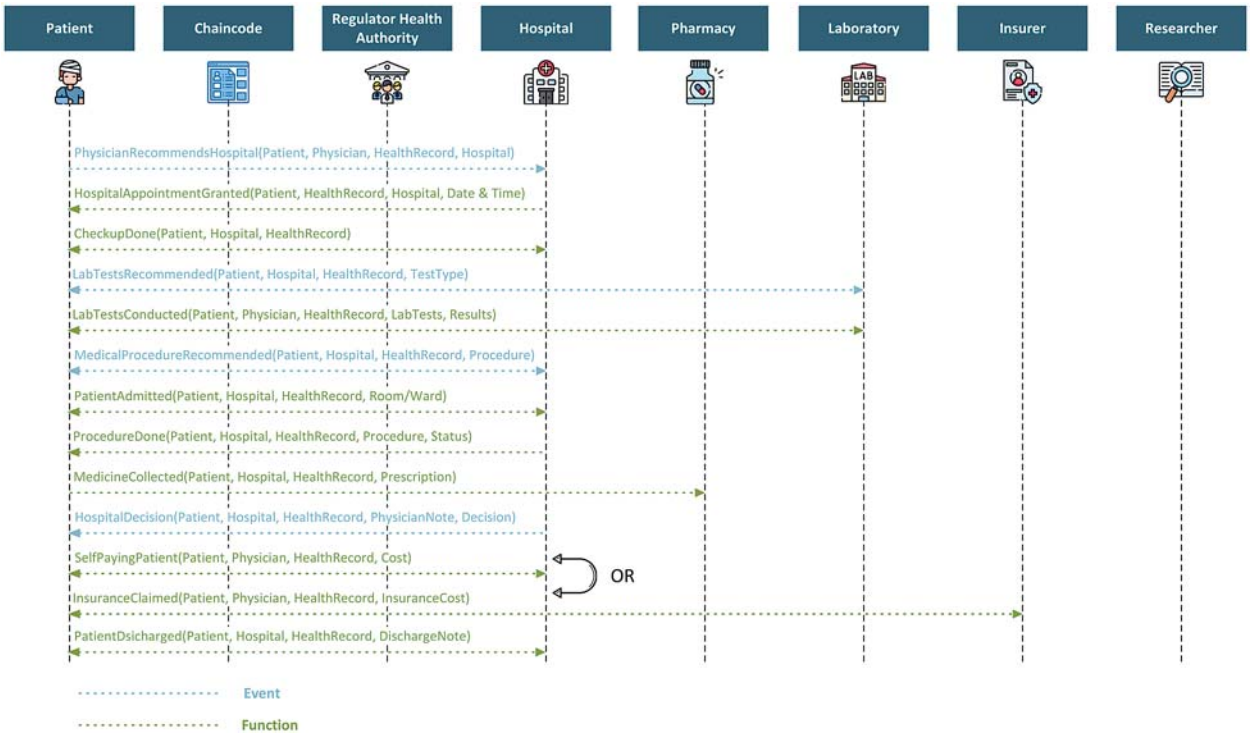

Figure 8: Transaction process flow between patient and hospital

Data Standardization and Scope: It is significant for organizations to cater to what type of data will be stored on the blockchain ledger and how it will be stored, i.e. on-chain or off-chain storage. For healthcare EHRs, the majority of the patient data is private data and must be stored and verified against on-chain hash evidence. One of the significant aspects of data standardization is the size of the data stored on the ledger. Storing unimportant data on the ledger creates additional large transaction sizes that will affect the efficiency and performance of the blockchain [52]. To standardize the data stored on the blockchain ledger to achieve better efficiency and performance, enterprises need to align and adequately define the size, type and format of the data stored at the blockchain ledger. Furthermore, restricting the access to the blockchain network also helps in standardizing the data stored and exchanged on the network.

Adoption and Enticements for Stakeholders: Incentives and motivations are utmost necessary for blockchain-enabled systems to succeed. To perform and execute an EHR transaction on the blockchain network, we need to create a peer-to-peer network of interconnected nodes that enables computing power required to accomplish and process the submitted transaction on the ledger network. Furthermore, additional support can be provided for the adoption of private

permissioned blockchains. Different organizations are already implementing and testing the technology to track and trace the medical records and claims of individual patients and hospitals. This process incentivizes healthcare service providers to switch to electronic health records, and it increases the adoption and facilitates global blockchain-enabled health exchange system.

Costs of Operating Blockchain Technology: As blockchain technology enables us to provide efficient and well-organized systems for performing real-time transactions, finding and choosing the best-suited blockchain platform is not an easy task as the majority of the solutions are not fully developed. Implementation, energy and operating costs are one of the leading challenges faced by enterprises as the costs of running and implementing private permissioned blockchain systems are yet to be known to enable the efficient management of EHRs [53]. The existing platforms and legacy software systems are inefficient and centralized while executing the transactions causing massive implementation and maintenance costs. Blockchain's open-source technology, properties, and distributed nature can help reduce the operating and management cost. As blockchain is an immutable and transparent technology, the storage, backups and recovery become obsolete and gratuitous, along with the abolishing of data exchange integration points and time-consuming reporting activities.

Regulatory Consideration and Compliance: Healthcare policymakers need to consider and develop different healthcare policies, and guidelines regarding blockchain technology implications and insinuations such as the distributed storage, ownership of blocks and records in the ledger and when does this ownership change, along with different access permissions and rights on the blockchain network [54]. The healthcare industry needs to genuinely collaborate and facilitate with existing regulatory frameworks such as HIPPA framework for privacy and interoperability for the development and evolution of the healthcare ecosystem to formulate new administration policy objectives.

7 Conclusion

In this paper, we discussed how blockchain technology could be leveraged to improve and enrich the existing EHRs systems in healthcare. We proposed a Hyperledger Fabric Architecture for the secure and efficient management of EHRs systems. It enables us to create a private permissioned peer-to-peer blockchain network of various identified and registered healthcare stakeholders to achieve maximum interoperability, security, privacy, scalability, and permissioning. The other aspects of the paper lie in the illustration and discussion of functional transaction activities and events performed between various stakeholders such as patient, primary physician and hospital. In the future work, we are planning to implement the proposed blockchain architecture as it demands a lot of coding and professional technical details as the existing hyperledger fabric architecture 2.0 is too new and not very much stable to be easily implemented.

Funding Statement: This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] E. Jamoom, N. Yang and E. Hing, "Adoption of certified electronic health record systems and electronic information sharing in physician offices: United States, 2013 and 2014," *NCHS Data Brief 2016*, vol. 236, pp. 1–8, 2016.

[2] ISO, ISO/TR 18638:2017, *Health informatics—Guidance on health information privacy education in healthcare organizations*, 2017. June 1. [Online]. Available: https://www.iso.org/standard/63100.html (Accessed 15 October 2020).

[3] P. Yadav, M. Steinbach, V. Kumar and G. Simon, "Mining electronic health records (EHRs) A survey," *ACM Computing Surveys*, vol. 50, no. 6, pp. 1–40, 2018.

[4] S. Wass and V. Vimarlund, "Same, same but different: Perceptions of patients' online access to electronic health records among healthcare professionals," *Health Informatics Journal*, vol. 25, no. 4, pp. 1538–1548, 2019.

[5] J. P. New, D. Leather, N. D. Bakerly, J. McCrae and J. M. Gibson, "Putting patients in control of data from electronic health records," *BMJ*, vol. 360, pp. j5554, 2018.

[6] E. W. Ford, B. W. Hesse and T. R. Huerta, "Personal health record use in the United States: Forecasting future adoption levels," *Journal of Medical Internet Research*, vol. 18, no. 3, pp. 1–8, 2016.

[7] M. A. Alyami and Y. Song, "Removing barriers in using personal health record systems," in *2016 IEEE/ACIS 15th Int. Conf. on Computer and Information Science*, Okayama, pp. 1–8, 2016.

[8] T. Heart, O. Ben-Assuli and I. Shabtai, "A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy," *Health Policy and Technology*, vol. 6, no. 1, pp. 20–25, 2017.

[9] C. Showell, "Barriers to the use of personal health records by patients: A structured review," *PeerJ*, vol. 5, pp. e3268, 2017.

[10] G. Iacobucci, "Cervical screening: GP leaders slam capita over failure to send up to 48,500 letters," *BMJ*, vol. 363, pp. k4832, 2018.

[11] CRICO, "CRICO Strategies, 2015 Annual Benchmarking Report," *Malpractice risks in communication failures*, 2015. December 30. [Online]. Available: https://www.rmf.harvard.edu/Malpractice-Data/Annual-Benchmark-Repo (Accessed 10 October 2020).

[12] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla and K. Shuaib, "Introducing blockchains for healthcare," in *Int. Conf. on Electrical and Computing Technologies and Applications*, Ras Al Khaimah, United Arab Emirates, 2017.

[13] L. L. Fragidis and P. D. Chatzoglou, "Development of nationwide electronic health record (NEHR): An international survey," *Health Policy and Technology*, vol. 6, no. 2, pp. 124–133, 2017.

[14] HIPAA guide, "The HIPAA Guide c2017," *HIPAA compliance guide (healthcare compliance)*, 2017. December 30. [Online]. Available: https://www.hipaaguide.net/hipaa-compliance-guide/ (Accessed 5 October 2020).

[15] NHS, "The NHS long term plan," 2019. [Online]. Available: https://www.longtermplan.nhs.uk/wp-content/uploads/2019/08/nhs-long-term-plan-version-1.2.pdf.

[16] L. Chen, W. K. Lee, C. C. Chang, K. K. Choo and N. Zhang, "Blockchain based searchable encryption for electronic health record sharing," *Future Generation Computer Systems*, vol. 95, pp. 420–429, 2019.

[17] N. Akpan, "Has health care hacking become an epidemic?," 2016. [Online]. Available: https://www.pbs.org/newshour/science/has-health-care-hacking-become-an-epidemic (Accessed 5 October 2020).

[18] U.S. Department of Health, "Breaches affecting 500 or more individuals," 2017. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (Accessed 15 October 2020).

[19] W. Smart, "Lessons learned review of the WannaCry Ransomware Cyber Attack," 2018. [Online]. Available: https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf (Accessed 15 October 2020).

[20] A. Morse, "Investigation: WannaCry cyber-attack and the NHS," 2018. [Online]. Available: https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (Accessed 15 October 2020).

[21] T. T. Kuo, H. F. Kim and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, 2017.

[22] A. K. Clauson , E. A. Breeden, C. Davidson and T. K. Mackey, "Leveraging blockchain technology to enhance supply chain management in healthcare: An exploration of challenges and opportunities in the health supply chain," *Blockchain in Healthcare Today*, vol. 1, no. 3, pp. 1–2, 2018.

[23] L. Castaldo and V. Cinque, "Blockchain-based logging for the cross-border exchange of e-health data in Europe, " in *International ISCIS Security Workshop*. Cham: Springer, pp. 46–56, 2018.

[24] 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, no. 10, pp. 218, 2016.

[25] 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.

[26] K. Fan, S. Wang, Y. Ren, H. Li and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 136, 2018.

[27] 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," *Journal of Medical Systems*, vol. 42, no. 8, pp. 147, 2018.

[28] B. Shen, J. Guo and Y. Yang, "MedChain: Efficient healthcare data sharing via blockchain," *Applied Sciences*, vol. 9, no. 6, pp. 1207, 2019.

[29] L. Zhu, Y. Wu, K. Gai and K. K. Choo, "Controllable and trustworthy blockchain-based cloud data management," *Future Generation Computer Systems*, vol. 91, pp. 527–535, 2019.

[30] P. Genestier, S. Zouarhi, P. Limeux, D. Excoffier, A. Prola *et al.,* "Blockchain for consent management in the e-health environment: A nugget for privacy and security challenges," *Journal of the International Society for Telemedicine and eHealth*, vol. 5, pp. GKR–e24, 2017.

[31] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 152, 2018.

[32] A. Al Omar, M. Z. Bhuiyan, A. Basu, S. Kiyomoto, S. M. *et al.,* "Privacy-friendly platform for healthcare data in cloud based on blockchain environment," *Future Generation Computer Systems*, vol. 95, pp. 511–521, 2019.

[33] J. Huang, Y. W. Qi, M. R. Asghar, A. Meads and Y. C. Tu, "MedBloc: A blockchain-based secure EHR system for sharing and accessing medical data," in *2019 18th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications/13th IEEE Int. Conf. on Big Data Science and Engineering*, Rotorua, New Zealand, pp. 594–601, 2019.

[34] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *21st Euromicro Conf. on Digital System Design*, pp. 699–706, 2018.

[35] X. Zhang, S. Poslad and Z. Ma, "Block-based access control for blockchain-based electronic medical records (EMRs) query in eHealth," in *IEEE Global Communications Conf.*, pp. 1–7, 2018.

[36] P. Zhang, J. White, D. C. Schmidt, G. Lenz and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalable share clinical data," *Computational and Structural Biotechnology Journal*, vol. 16, pp. 267–278, 2018.

[37] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma *et al.,* "Blochie: A blockchain-based platform for healthcare information exchange," in *2018 IEEE Int. Conf. on Smart Computing*, Taormina, Italy, pp. 49–56, 2018.

[38] K. Peterson, R. Deeduvanu, P. Kanjamala and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, pp. 1–10, 2016.

[39] S. Badr, I. Gomaa and E. Abd-Elrahman, "Multi-tier blockchain framework for IoT-EHRs systems," *Procedia Computer Science*, vol. 141, pp. 159–166, 2018.

[40] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 140, 2018.

[41] R. Guo, H. Shi, Q. Zhao and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.

[42] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du *et al.,* "MeDShare: Trustless medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[43] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in *AMIA Annual Symp. Proc.*, Bethesda MD, USA, pp. 650, 2017.

[44] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. Tavares *et al.,* "A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform," *Cognitive Systems Research*, vol. 52, pp. 1–11, 2018.

[45] X. Zhang and S. Poslad, "Blockchain support for flexible queries with granular access control to electronic medical records (EMR)," in *2018 IEEE Int. Conf. on Communications*, Kansas City, MO, USA, pp. 1–6, 2018.

[46] L. Bell, W. J. Buchanan, J. Cameron and O. Lo, "Applications of blockchain within healthcare," *Blockchain in Healthcare Today*, vol. 1, no. 1, pp. 1–7, 2018.

[47] IBM, "Health rallies for blockchains: Keeping patients at the center," 2016. [Online]. Available: https://www.ibm.com/downloads/cas/BBRQK3WY (Accessed October 2020).

[48] A. Bessani, J. Sousa and M. Vukolić, "A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform," in *Proc. of the 1st Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers*, Las Vegas, NV, USA, pp. 1–2, 2017.

[49] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis *et al.,* "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. of the Thirteenth EuroSys Conf.*, pp. 1–15, 2018.

[50] Hyperledger, "Hyperledger/Fabric," GitHub, 2020. [Online]. Available: https://github.com/hyperledger/fabric (Accessed July 2020).

[51] P. Sylim, F. Liu, A. Marcelo and P. Fontelo, "Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention," *JMIR Research Protocols*, vol. 7, no. 9, pp. e10163, 2018.

[52] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson *et al.,* "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *Journal of Medical Systems*, vol. 42, no. 7, pp. 130, 2018.

[53] G. G. Dagher, J. Mohler, M. Milojkovic and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustainable Cities and Society*, vol. 39, pp. 283–297, 2018.

[54] T. Alshalali, K. M'Bale and D. Josyula, "Security and privacy of electronic health records sharing using hyperledger fabric," in *2018 Int. Conf. on Computational Science and Computational Intelligence*, Las Vegas, NV, USA, pp. 760–763, 2018.