2025 IEEE/ACM 7th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB) | 979-8-3315-0194-5/25/$31.00 ©2025 IEEE | DOI: 10.1109/WETSEB66605.2025.00010

HealthChain: A Blockchain-Based Framework for Electronic Health Record Management System

Mashiat Amin Farin*, Sampad Sikder*, Ashabul Yamin Raad†, Meah Tahmeed Ahmed‡, Tahlil Tahlil§
*Institute of Information Technology, University of Dhaka, Bangladesh, Email: bsse1202@iit.du.ac.bd, bsse1219@iit.du.ac.bd
†Department of Computer Science and Engineering, BRAC University, Bangladesh, Email: yamin.raad6109@gmail.com
‡University of Texas at Dallas, USA, Email: meah.ahmed@utdallas.edu
§Tero Labs LLC, USA, Email: tahlil@ieee.org

***Abstract*—Electronic health management systems (EHMS) play a crucial role in modern healthcare. They store important medical information such as patients' medical histories, treatment plans, and diagnostic reports. However, the current EHMS landscape faces numerous challenges. These challenges hinder efficient data management, and collaboration among stakeholders, and compromise patient privacy and data security. Blockchain technology offers a promising solution to address these issues. By leveraging its decentralized and immutable nature, blockchain can create a secure, transparent, and tamper-resistant platform for storing, managing, and sharing electronic health records. This paper proposes an end-to-end solution called Healthchain based on a private permissioned blockchain network. Healthchain uses the Istanbul Byzantine fault tolerance (IBFT) consensus algorithm to reduce computation costs and increase speed. Secure multiparty computation allows medical data monetization without compromising privacy or data authenticity (ensured by blockchain) along with Zero knowledge proof and differential privacy for researchers. HealthChain also uses an efficient method for storing medical reports using IPFS, reducing the burden on single storage. It creates awareness about privacy issues and creates awareness about social engineering attacks based on the project. This paper explains the proposed framework, comparing performance with existing traditional and digital systems, and considers Bangladesh as an example to test its viability.**

***Index Terms*—Electronic Health Management System (EHMS), Healthcare, Blockchain, Hyperledger Besu, IPFS, Access Control**

I. Introduction

Health is arguably the most vital element of life. Nations like Denmark, Norway, and Switzerland, leaders in the LPI rankings, have emphasized the importance of maintaining thorough medical records for precise diagnosis and treatment [1]. The COVID-19 crisis has heightened the significance of vaccinations and record-keeping. While Denmark, ranked 1st in 2020, has commenced vaccine tracking, it only began in 2015, leaving earlier data unavailable.

Healthcare data frequently fall prey to breaches. Between 2009 and 2021, 4,419 breaches involving 500 or more records were reported, compromising 314,063,186 records—94.63% of the 2021 U.S. population. From 2018 to 2021, breach rates have doubled, with an average of 1.95 significant breaches per day in 2021 [2].

These breaches highlight an urgent need for innovative ways to improve data security and interoperability in electronic health management systems (EHMS). EHMS is crucial for storing medical histories, treatment plans, diagnostics, and other vital information. However, they grapple with challenges such as breaches [3], poor interoperability [4][5][6], inefficient data sharing, and limited patient data control [7][8]. Addressing these issues requires solutions that enhance security, facilitate information sharing, and empower patients.

In this context, blockchain technology presents a transformative opportunity to revolutionize EHMS. Its decentralized and immutable nature ensures secure and transparent storage, management, and sharing of health records. Through cryptographic techniques and smart contracts, blockchain ensures data integrity, mitigates unauthorized access, and empowers patients. Additionally, its inherent trust and transparency foster collaboration among stakeholders, leading to improved healthcare outcomes and reduced administrative burdens.

This paper presents an end-to-end solution for an EHMS based on a private permissioned blockchain network. The blockchain is created using Hyperledger Besu, addressing the challenges faced by traditional healthcare data management systems and mitigating issues such as fragmented health records and services. The proposed solution, Healthchain, utilizes cryptographic principles to create tamper-proof logs of health records and employs smart contracts to automate event recording.

II. Related Work

A. Digital Centralized Approaches

Various digitized health record systems are proposed in the literature, including centralized and decentralized approaches.Storing medical records within a centralized system that is interoperable across different hospitals presents a significant challenge. However, potential solutions have been suggested. In 2017, Roehrs et al. introduced a distributed model called OmniPHR, incorporating personal health records for patients and healthcare providers [9]. Additionally, in 2010, they proposed a cloud computing solution for hospital information systems, streamlining construction, enabling information sharing, and allowing for high-end processing within the ”cloud”. These proposed solutions hold promise in addressing the challenge of achieving a comprehensive view

979-8-3315-0194-5/25/$31.00 ©2025 IEEE
DOI 10.1109/WETSEB66605.2025.00010

of a patient's health history and providing healthcare providers with real-time patient data.

B. Blockchain Based Approaches

There have been suggestions to utilize blockchain and IPFS technologies for decentralized health record storage systems. A proposal made by A. Azaria suggests the use of smart contracts on the Ethereum Blockchain network to regulate permissions and control access to medical records (Azaria et al., 2016) [10]. Liang X et al. (2017) have proposed the integration of blockchain with mobile applications to enable data sharing with healthcare providers and insurance companies [11]. They have employed Hyperledger Fabric for access control and integrity. Ancile is another framework that uses the permissioned Ethereum-based blockchain Quorum for access control management and interoperability in electronic health records [12]. Sawant (2022) propose blockchain-based systems for decentralized and secure electronic health record (EHR) storage [17]. Kumar (2021) presents a comparative analysis of existing IPFS and blockchain-based healthcare storage solutions [13]. Here, they propose a distributed off-chain storage system for medical data using IPFS and blockchain technology. This system ensures patient privacy and enables authorized access to medical data. These papers collectively suggest that decentralized health record storage systems enhance data security, accessibility, and privacy. Kazira Abeg (2019) proposes BlockMedCare, a scalable solution that integrates IoT and blockchain technologies for storing medical records [15]. Yang (2020) proposes a decentralized system for managing medical data using blockchain, with a focus on protecting data privacy during data sharing [18]. Chamola (2022) suggests an AI-assisted blockchain-based framework for secure electronic medical record (EMR) management [19]. Mohsan (2022) describes a proof-of-concept architecture for a distributed patient-centric test report and image management system [20]. Taylor (2022) suggests VigilRx for managing medical prescriptions using smart contracts [14]. Islam (2023) proposes a distributed healthcare application platform for Bangladesh [16]. These papers collectively demonstrate that decentralized solutions utilizing blockchain and distributed file systems enable secure and efficient management of medical electronic reports while preserving patient privacy and control. Table - 1 presents a comparative analysis of these solutions.

These papers collectively suggest that decentralized solutions using blockchain and distributed file systems can provide secure and efficient management of medical electronic reports while preserving patient privacy and control. For Bangladesh, a robust and scalable framework is essential, allowing a significant number of patients to store extensive amounts of data while ensuring the system operates efficiently and smoothly. HealthChain offers a transformative, context-aware framework specifically designed to tackle the healthcare challenges in Bangladesh. It combines scalability, privacy, and cost-efficiency to address critical gaps in electronic health management.

III. Problem Formulation

Electronic health management systems (EHMS) in Bangladesh currently face several obstacles in data management, stakeholder collaboration, and patient privacy and security. Traditional EHMS encounter issues like data breaches, poor interoperability, repeated tests, delayed diagnoses, and restricted patient control. These highlight the need for a new approach to create secure, transparent, and patient-focused data handling.

Data Breaches and Privacy Concerns: Existing EHMS have vulnerabilities that lead to data breaches and unauthorized access, threatening patient privacy. High-profile cases stress the need for better data security.

Interoperability Issues: The inability of EHMS platforms to interoperate obstructs data exchange and collaboration among providers, resulting in fragmented patient records and inefficiencies in care.

Redundant Tests and Slow Processes: Without a centralized medical repository, all parties face redundant testing, diagnosis delays, longer treatment cycles, and increased costs.

Limited Patient Control: Patients have limited control over their health data, impacting access, management, and information sharing with healthcare providers and researchers.

Inefficient Insurance Claim Processing: Complex billing and opaque insurance claims lead to administrative inefficiency, delayed payments, and increased costs.

Fragmented Healthcare Ecosystem: Lack of cooperation among healthcare entities hampers effective delivery of care.

Bureaucratic Procrastination: Delays in insurance claims disrupt care and system operations.

Lack of Data-driven Insights: The absence of a centralized EHMS restricts access to comprehensive data, limiting research and treatment strategies.

Lack of Transparency: Identifying issues is difficult due to counterfeit reports and lack of transparency, affecting diagnoses and processes.

Technological Bottlenecks: Slow technology adoption presents persistent challenges.

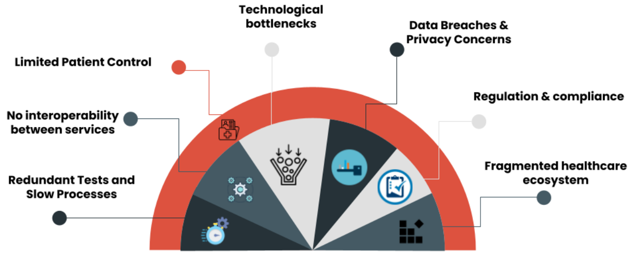

Technological bottlenecks
Data Breaches & Privacy Concerns
Limited Patient Control
Regulation & compliance
No interoperability between services
Fragmented healthcare ecosystem
Redundant Tests and Slow Processes

Fig. 1: Challenges faced by the current system

Given these challenges, this paper suggests a blockchain-based solution focusing on security, transparency, and patient-centeredness. Using blockchain's features, it aims to transform EHMS with data immutability, greater security, streamlined operations, and patient empowerment.

TABLE I: Comparison of Blockchain Solutions

Name	Blockchain	EVM Support	Consensus	Network Type	Data Storage	Data Encryption	Access Control	Transaction cost	Scalability
MedRec [10]	Ethereum	Yes	PoW	Permissionless	Centralized DB	No	Yes	High	Yes
Liang X. et Al [11]	Hyperledger Fabric	No	PBFT	Permissioned	centralized DB	No	Yes	Zero	Yes
Ancile [12]	Quorum	Yes	QuorumChain	Permissioned	centralized DB	Yes	Yes	Zero	No
Kumar (2020) [13]	Not specified		PoW	Permissioned	IPFS	No	No		
VigilRx [14]	Ethereum	Yes	Not specified	Permissionless	centralized DB	Yes	No	High	Yes
BlockMedCare [15]	Ethereum	Yes	PoA	Permissioned	IPFS	Yes	Yes	High	Yes
Islam (2023) [16]	Hyperledger fabric	No	Raft	Permissioned	IPFS	No	Yes	Zero	Yes
Our system	Hyperledger Besu	Yes	PoA	Permissioned	IPFS	Yes	Yes	Zero	Yes

The aim is to lay out a plan for transforming healthcare data management via blockchain. By tackling these challenges, it seeks to boost patient care, improve efficiency, and enhance cooperation in the healthcare ecosystem.

IV. Methodology

HealthChain is a private permissioned blockchain network that utilizes Hyperledger Besu as its Distributed Ledger Technology. Besu is a Java-based Ethereum client that implementings the Enterprise Ethereum Alliance (EEA) and can run onoperate on both public and private networks, as well as testnets [21]. Besu is compatible with Ethereum smart contracts, allowing for seamless integration with the Ethereum blockchain.

Kaleido offers a blockchain-as-a-service architecture that implements a "permissioned" version of the Ethereum protocol. This means that member participants in Kaleido's network operate with authenticated identities supported by digital certificate chains [22]. By incorporating their blockchain-as-a-service model into Hyperledger Firefly, Kaleido has created a centralized deployment hub for decentralized applications [23]. With the release of Hyperledger Firefly 1.1, users have access to a complete technology stack for building and scaling Web3 applications. We utilize Hyperledger Firefly to integrate our smart contracts with front-end applications. Since Besu is an Ethereum-based private blockchain network, it supports contracts written in solidity. These contracts are deployed on the blockchain network and can be invoked using the contract's Application Binary Interface (ABI). Hyperledger Firefly provides a contract interface that allows for contract invocation through HTTP API requests. The HTTP API requests are based on the OpenAPI specification and can be interacted with using the Swagger UI. This provides an easy-to-use REST API for seamless interaction between the frontend and the blockchain.

To ensure data privacy, a private IPFS network is utilized to store data in a way that only designated peers on the network can access it. IPFS content-based addressing also enhances the speed of data transfers [24]. Almost all IPFS frameworks stores data by encryption and has proper key managmeent techniques. For healthchain, we are implementing Pinata IPFS. Hyperledger Firefly provides a gateway to connect with IPFS, which handles off-chain file data required to support on-chain data. For instance, diagnostic reports may contain images that, if stored on-chain, would cause the chain to grow rapidly. Therefore, it is considered ideal to store the hash of the image information on-chain while storing the actual image off-chain on IPFS.

Besu supports two node types: full nodes and archive nodes. Full nodes store the latest information on the blockchain, while archive nodes maintain a complete copy of the chain from Genesis. In Hyperledger Firefly, nodes hold a full copy of the blockchain.

Currently, the network is configured with four archive nodes. In Hyperledger Besu, full nodes serve as validator nodes. Validator nodes are randomly selected from the archive nodes. Full nodes should be set up in all major public (both national and district level) and large private hospitals in Bangladesh. The permissions are also defined based on the type of node. The user application monitors and records transactions on health data assets. Therefore, they function like wallets where user access control is managed. The archive nodes include all major public hospitals, the Ministry of Health, and some other national-level specialized hospitals such as BIRDEM, NINS & H, NIKDU, NICVD, NIO, NIMH, etc. [25].

For testing purposes, smart contracts were deployed to a local firefly node running Hyperledger Besu. A node server was set up with 10 patients and 10 doctors for testing. The blockchain server consisted of four full nodes, which also acted as validator nodes. Performance was evaluated using two approaches: stacking data without clearing previously pushed data, and removing previously pushed data. There was no significant difference in timings between the two methods. However, write times increased as the data volume increased, while read times improved with more data pushed to the blockchain.

V. Solution Framework

A. Hyperledger Firefly Overview

Hyperledger FireFly serves as an organization's gateway to Web3, encompassing all the blockchain ecosystems in which they participate. With Hyperledger, users gain access to a central hub for managing all Web3 connections. This allows for various functionalities, such as tokenized value transfer, invoking different types of smart contracts, indexing blockchain data, triggering events in applications and back-office systems, managing NFTs, and utilizing a private address book for managing signing addresses and relationships. Additionally, the Firefly UI Sandbox is used for deploying smart contracts on the blockchain network, while the REST API provided by Firefly enables the invocation of these deployed smart contracts.

Kaleido offers a blockchain-as-a-service architecture through Hyperledger Firefly. User authentication and access control are maintained by the Firefly nodes, using the identify plugin. For custom identity management, Firefly recommends utilizing the identity plugin [26]. Firefly generates a new private key and address for users to utilize, encrypting the private key and storing it in the signing container. Each user must be registered under a network node, with permitted users including doctors, diagnostic centers, and patients. The provided key serves as the validation scheme. The custom identity plugin operates based on the W3C standard for Decentralized Identifier (DID) and is saved on Hyperledger Besu.

B. Technical Architecture

HealthChain utilizes the PoA (IBFT 2.0) consensus protocol of Hyperledger Besu. Compared to the Ethash proof of work consensus protocol used on the Ethereum Mainnet [27], PoA consensus protocols offer faster block times and greater transaction throughput. HealthChain is a blockchain-based technology that employs an Istanbul Byzantine Fault Tolerant System (IBFT), which ensures a single agreed-upon ordering for transactions in a permissioned network [28]. This is made possible by utilizing Hyperledger Besu as the underlying technology, which implements the ”Proof of Authority” consensus algorithm based on IBFT 2.0.

IBFT provides the following benefits:

1) **Immediate block finality:** Only 1 block can be proposed at a given chain height.
2) **Reduced time between blocks:** The time required to validate a block is significantly less compared to proof of work.
3) **High data integrity and fault tolerance:** IBFT consensus is fault tolerant up to 33.33% of nodes.
4) **Operational flexibility:** The group of validators can be modified over time, ensuring that only trusted nodes are involved in the validation process.

IBFT 2.0 improves upon IBFT 1.0 in two areas. Firstly, it increases the number of nodes required to reach a quorum. For example, IBFT 2.0 requires 4 out of 5 nodes to reach an agreement, whereas IBFT 1.0 only requires 3. This change prevents a Byzantine validator from influencing different blocks by getting two sets of honest validators to agree on different outcomes. Secondly, an enhanced round change protocol guarantees that if any validator commits in a round, the proposed block in any subsequent rounds will match the committed block.

The health app consists of two components: the interoperable application and the blockchain itself. The health application is designed to cater to the public and incorporates various design elements that abstract the backend operations to provide a seamless user experience. To ensure interoperability across devices, the front end is built using the ReactJS framework. Figure 2 illustrates the high-level architecture. Hyperledger Besu is well-suited for this scenario as it allows for both node permissions and account permissions through the use of smart contracts.

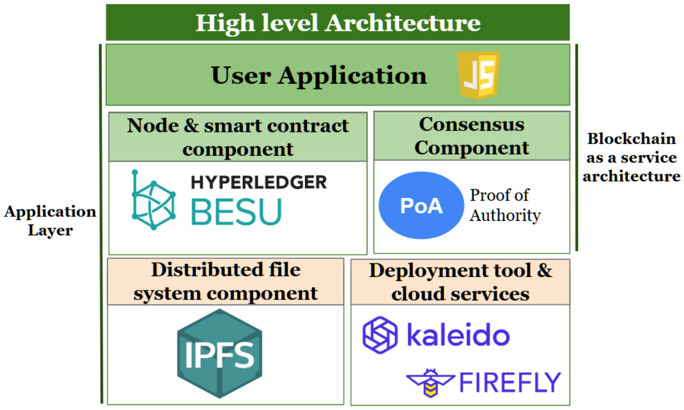

High level Architecture
User Application
JS
Node & smart contract component
HYPERLEDGER BESU
Consensus Component
PoA
Proof of Authority
Blockchain as a service architecture
Application Layer
Distributed file system component
IPFS
Deployment tool & cloud services
kaleido
FIREFLY

Fig. 2: High level architecture of HealthChain

The Firefly REST API is used to call the deployed smart contracts. Hyperledger Firefly supports version control and identity management for smart contracts in the network. The identities provide the necessary digital signatures for stakeholders.

One of the big concerns is a large user base and lots of medical data being constantly added can cause reading and writing on the network to become slow. Hyperledger besu previously used forest of tries to store ethereum’s complex and vital states.[18] These states can grow increasingly large and synchronization becomes a challenge. Recently, besu merged with bonsai tries which uses better pruning, reduced disk usage, faster synchronization of nodes and reduction of the client running “blocks behind the network”. Bonsai improves state storage size significantly.

Kaleido provides the blockchain as a service architecture through Hyperledger Firefly. User authentication & access control is maintained by the firefly nodes, through the identify plugin. For custom identity, firefly recommends using the identity plugin. [33] Firefly creates a new private key & address for users to be able to use, & it loads the encrypted private key into the signing container. Each user needs to be registered under a node of the network. The key they are provided with serves as the validation scheme. The access control of user is defined in the Decentralized identity (DID). The custom identity plugin operates on DID defined by W3C standard and saved on Hyperledger Besu.

The patient’s health record is considered an asset. The initial digitized data is stored in Hyperledger Besu through smart contracts. Assets are registered or created when new health records are inserted (new transactions). Figure 3 provides insight into how the system’s interactions are achieved.

Data is uploaded using the shared data plugin of Hyperledger Firefly. The data object is uploaded through a REST

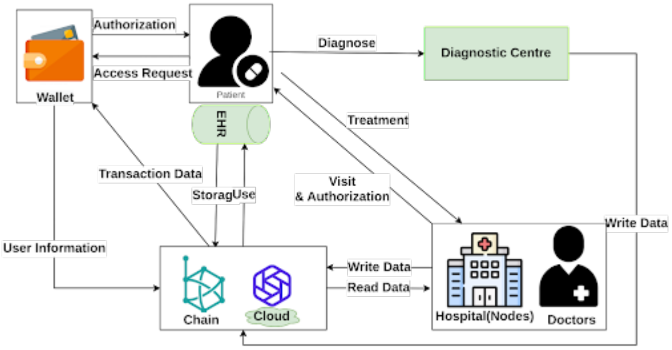


Fig. 3: Governance overview of HealthChain

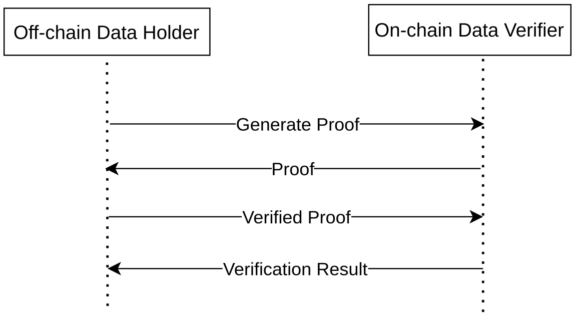


Fig. 4: zk-SNARK process

endpoint. A message is then broadcasted to all nodes and the data blob is published on the shared IPFS storage. The content ID of the data is stored on the blockchain.

1) Zero Knowledge Proof: Patient information and records are stored on chains. While efforts have been made to avoid storing sensitive data on the chain, storing medical records and patient IDs can still reveal important information to interested parties. To protect the privacy of this data, a zero knowledge proofing mechanism is implemented.

We have utilized a zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) circuit developed using Zokrates to enforce the zero knowledge proof. This circuit verifies chain data without revealing sensitive information. Zokrates is used to generate proving and verification keys, and a smart contract ensures the verification of on-chain data. On the blockchain, the verifier smart contract uses the verification keys to verify the proof.

In this system, medical records are stored securely off-chain in an IPFS network. A unique hash is created for each record, using a cryptographic hash function like SHA-256. The hash of each medical record is then stored on-chain, serving as proof of its existence without disclosing any sensitive information.

Next, Zokrates is utilized to generate a zk-SNARKs proof, which verifies the integrity of the medical record without revealing the actual record itself. This proof can be verified on-chain using the verification keys generated by Zokrates. A verifier contract is responsible for enforcing the proof on the blockchain. The verifier accomplishes this by comparing the hash digest provided on-chain with the one off-chain. The basic circuit written in Zokrates ZSL is as follows:

```
def main(private field[256] a, field[256]
    b) -> (field):
    field result = 1
    for field i in 0..256 do
        result = if a[i] == b[i] then
            result else 0 fi
    endfor
    return result
```

In this program, a and b are private inputs, each representing a 256-bit hash. The program checks if all bits of a and b are equal, and returns 1 if true, 0 otherwise.

C. Data Architecture

In order to maintain a secure and efficient network, we utilize on-chain and off-chain read-write access control matrices, as outlined in Table 3 and Table 4. These matrices help to minimize network traffic, while ensuring immutability and transaction validation by active stakeholders, for both transactional and non-transactional data.

D. Smart Contract Design

Below are the functions of the smart contracts:

• **Doctor Contract:** Each doctor's registration smart contract (Doctor) will be stored in the blockchain, and they will be provided with a unique identifier. The inputs of the smart contracts are license number, doctorId, and name. Some functions include:

- addDoctor(): This function confirms the registration of the doctor by invoking it using the doctor's address. - getDoctor(): This function returns the doctor and their ID.

• **Diagnostic Center Contract:** Each Diagnostic Center is provided with a unique identifier.

- addCenter(): This function confirms the registration of the diagnostic center by invoking it using the Diagnostic Center's address.

- getDiagnosticCenter(): This function returns the diagnostic center contract and its ID.

• **Patient Contract:** Each patient is assigned a unique identifier. The smart contract (Patient) will be stored in the blockchain. Some functions include:

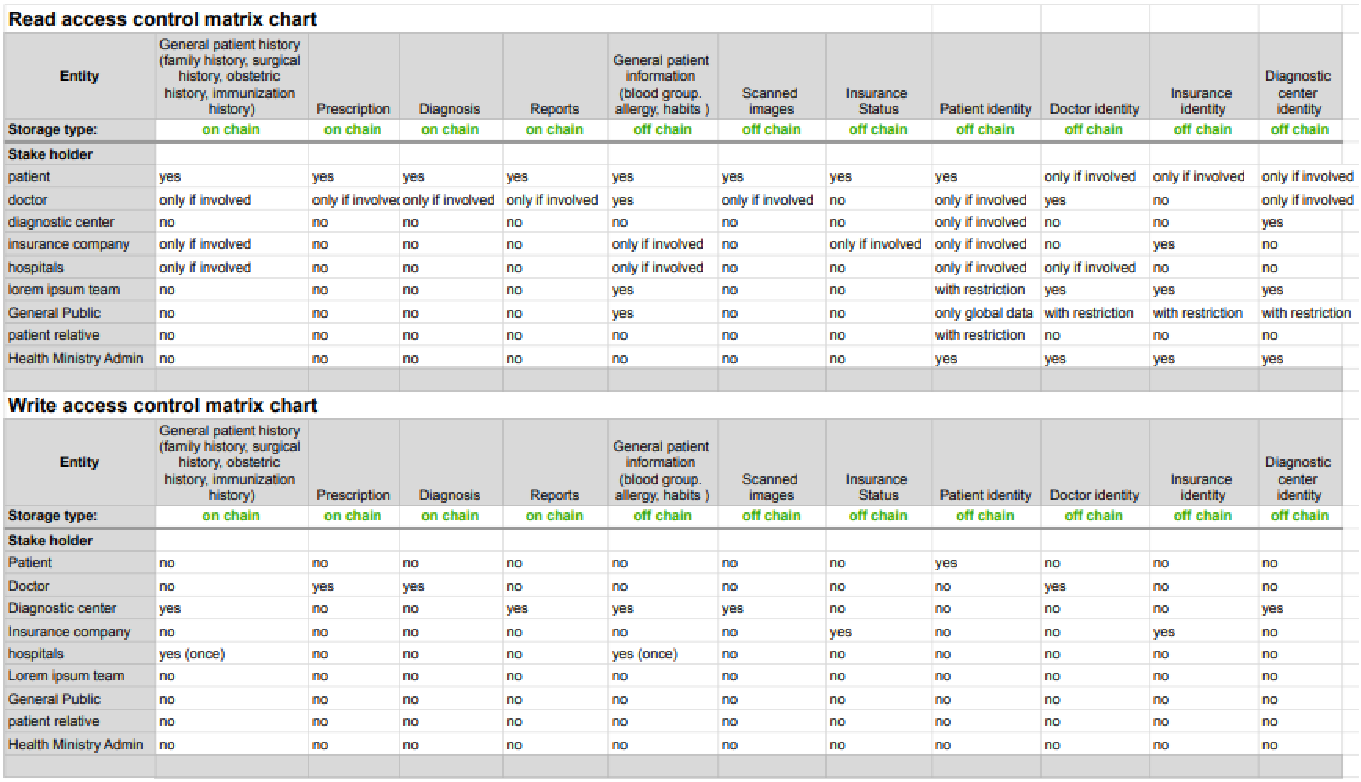
- addPatient(): This function confirms the registration of the patient. It stores the patient's name, national identity, and date of birth.

- getPatient(): This function returns the patient contract and its ID.

• **Health Record Contract:** Each health record is assigned a unique identifier. The smart contract (PatientRecord) will be stored in the blockchain. Some functions include:

- healthRecordStore(): This function confirms the identity of the patient and then stores their prescription record on the blockchain. It has the onlyDoctor() modifier.

- diagnosticReportStore(): This function stores the content ID of the prescription on the blockchain whenever a new



Read access control matrix chart

Entity	General patient history (family history, surgical history, obstetric history, immunization history)	Prescription	Diagnosis	Reports	General patient information (blood group. allergy, habits)	Scanned images	Insurance Status	Patient identity	Doctor identity	Insurance identity	Diagnostic center identity
Storage type:	on chain	on chain	on chain	on chain	off chain	off chain	off chain	off chain	off chain	off chain	off chain
Stake holder											
patient	yes	yes	yes	yes	yes	yes	yes	yes	only if involved	only if involved	only if involved
doctor	only if involved	only if involvec	only if involved	only if involved	yes	only if involved	no	only if involved	yes	no	only if involved
diagnostic center	no	no	no	no	no	no	no	only if involved	no	no	yes
insurance company	only if involved	no	no	no	only if involved	no	only if involved	only if involved	no	yes	no
hospitals	only if involved	no	no	no	only if involved	no	no	only if involved	only if involved	no	no
lorem ipsum team	no	no	no	no	yes	no	no	with restriction	yes	yes	yes
General Public	no	no	no	no	yes	no	no	only global data	with restriction	with restriction	with restriction
patient relative	no	no	no	no	no	no	no	with restriction	no	no	no
Health Ministry Admin	no	no	no	no	no	no	no	yes	yes	yes	yes

Write access control matrix chart

Entity	General patient history (family history, surgical history, obstetric history, immunization history)	Prescription	Diagnosis	Reports	General patient information (blood group. allergy, habits)	Scanned images	Insurance Status	Patient identity	Doctor identity	Insurance identity	Diagnostic center identity
Storage type:	on chain	on chain	on chain	on chain	off chain	off chain	off chain	off chain	off chain	off chain	off chain
Stake holder											
Patient	no	no	no	no	no	no	no	yes	no	no	no
Doctor	no	yes	yes	no	no	no	no	no	yes	no	no
Diagnostic center	yes	no	no	yes	yes	yes	no	no	no	no	yes
Insurance company	no	no	no	no	no	no	yes	no	no	yes	no
hospitals	yes (once)	no	no	no	yes (once)	no	no	no	no	no	no
Lorem ipsum team	no	no	no	no	no	no	no	no	no	no	no
General Public	no	no	no	no	no	no	no	no	no	no	no
patient relative	no	no	no	no	no	no	no	no	no	no	no
Health Ministry Admin	no	no	no	no	no	no	no	no	no	no	no

Fig. 5: Read-Write Access Control Matrix

prescription is added. - healthRecordGet(): This view function fetches the prescriptions of the patient.

- healthReportGet(): This view function fetches the diagnostic report of the patients.

The UML diagram of the smart contracts is mentioned in Figure - 6.

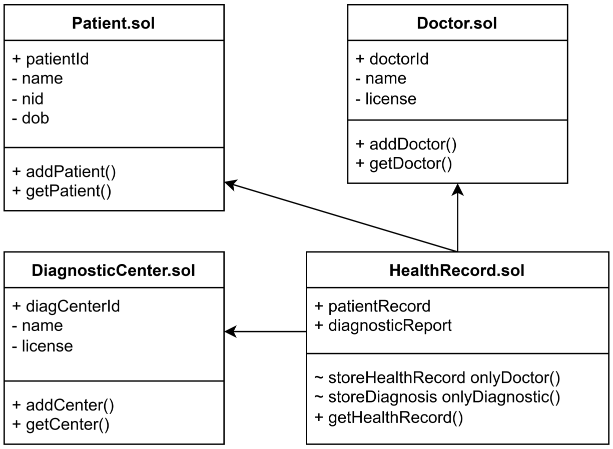


Fig. 6: UML Diagram

VI. Discussion

Our solution is designed to handle the healthcare sector in Bangladesh. The discussion section provides insights into how HealthChain compares to other similar solutions, why blockchain is an effective tool for maintaining health records, especially for a country with a large population like Bangladesh, and how our solution addresses security concerns. In Table 4, a range of alternative solutions present in this landscape can be observed. These solutions have been collected through our extensive literature review and have been assessed in terms of their respective attributes.

For performance analysis, we tested how much time it took Hyperledger Besu to read from the network with increasing number of records. To conduct the testing, we utilized a VM running Ubuntu 22.04 as the operating system. The VM was equipped with 8GB of RAM and a Ryzen 5 3600 processor, with 4 cores and 8 threads allocated specifically to the VM. Additionally, we created a local firefly supernode by deploying a docker image on the localhost. A node server was set up to conduct the test, configuring a total of 10 patients and 10 doctors. The blockchain server was established using four full nodes, which also acted as validator nodes.

Performance was measured using two approaches. The first approach involved stacking the data, where previously pushed data were not removed before pushing a new batch of data. The second approach involved removing the previously pushed data. There was no significant difference in the timings between the two methods.

We compared the block generation time with other permissioned blockchain networks. Hyperledger Fabric is a widely used private permissioned network. Fabric can support at most 20000 transactions where Besu supported upto 50000 on our system. The execution time of Besu was compared with that of the result of Hyperledger Fabric.

Execution time = Transaction placement time - Transaction completion time

The average execution time of Fabric and Besu was compared upto 20000 transactions. It was seen that Besu was much faster and with the increase of the number of transactions, Besu's performance was much better compared to Ethereum.

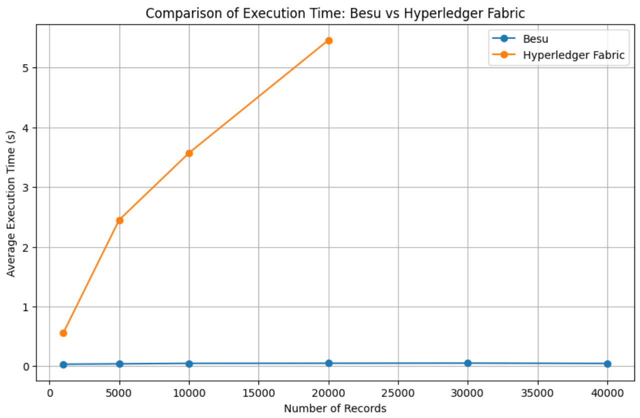


Fig. 7: Besu vs Hyperledger Fabric Execution Time Comparison

A secure system is crucial for maintaining the health records of a large number of patients. The major security objectives of the system are outlined below:

Confidentiality: In the proposed system, patient records are protected by digital signatures and are only accessible to authorized doctors. Diagnostic centers can store records but have limited access. All record transactions require patient approval.

Integrity: The proposed system ensures integrity by storing records on an immutable blockchain and securing transactions with digital signatures.

Accountability: Any individual performing a transaction on the blockchain can be traced on the network.

Access Control: A private permissioned blockchain network allows only authorized participants like hospitals and healthcare authorities to join. Patients undergo multi-factor authentication before being added, preventing data modification and limiting access to sensitive health data. The detailed access control and read write access is shown in Figure - 5.

Data Privacy: Only authorized entities can use smart contracts, and Zero Knowledge Proofs (ZKPs) enhance data privacy. ZKPs allow verification without revealing sensitive information, ensuring patient record confidentiality. HealthChain securely validates and executes transactions while keeping data encrypted and inaccessible to unauthorized parties. This comprehensive framework preserves data privacy and confidentiality withinlthChain ecosystem.

Scalability: The proposed system is highly scalable as it utilizes both on-chain and off-chain transaction methods. Large transactions, such as diagnostic images, are stored off-chain, with the chain keeping track of the corresponding IDs. Onboarding entities is seamlessly achieved using the firefly network.

Availability: The proposed system will be deployed through a blockchain network that supports Byzantine Fault Tolerance. This ensures that the system will function flawlessly even when 33.33% of the nodes are inactive.

Node Security: The random selection of validator nodes from archive nodes in Hyperledger Besu enhances security by preventing a single entity from having full control over consensus. It is highly resistant to a 51% attack.

In terms of file security and privacy, IPFS is responsible for managing off-chain file data that is essential for supporting on-chain data. Access to IPFS is limited to authorized nodes only. IPFS can be accessed using the plugin offered by Hyperledger Firefly, ensuring that only identifiable entities in the network can record transactions. To ensure the security of data stored on IPFS, it is encrypted and protected against any unauthorized access, including by network peers.

VII. Conclusion

The current EHMS landscape in Bangladesh faces several challenges, such as data breaches, privacy concerns, interoperability issues, redundant tests, slow diagnosis processes, limited patient control over health data, and inefficient insurance claim processing. These challenges call for a paradigm shift in the realm of EHMS.

This paper proposes a novel blockchain-based solution called Healthchain to address the aforementioned challenges and create a secure, transparent, and patient-centric healthcare data management system. It utilizes a combination of on-chain and off-chain storage to ensure data security and scalability. The smart contracts handle patient registration, health data management, access control, and audit trails. Healthchain offers a number of advantages over traditional EHMS solutions, including: data security, data privacy, transparency and accountability, patient control, interoperability and scalability.

The implementation of Healthchain is expected to have a number of benefits for the healthcare sector in Bangladesh, including: improving quality of care, reducing costs, increasing efficiency, and enhancing transparency and accountability.

Overall, Healthchain is a promising solution with the potential to revolutionize the healthcare sector in Bangladesh.

References

[1] LPI World Bank. *LPI rankings*. 2023. URL: https://lpi.worldbank.org/international/global.

[2] The HIPAA Journal. *Healthcare Data Breach Statistics*. 2024. URL: https://www.hipaajournal.com/healthcare-data-breach-statistics/.

[3] Fortune. *Hackers Don't Want Your Credit Card. They Want Your Medical Records*. 2018. URL: https://fortune.com/2018/03/20/hackers-dont-want-your-credit-card-they-want-your-medical-records/.

[4] Lipika Samal et al. “Care coordination gaps due to lack of interoperability in the United States: A qualitative study and literature review”. In: *BMC Health Services Research* 16 (Apr. 2016). DOI: 10.1186/s12913-016-1373-y.

[5] Amir Torab-Miandoab et al. “Interoperability of heterogeneous health information systems: a systematic literature review”. In: *BMC Medical Informatics and Decision Making* 23 (Jan. 2023). DOI: 10.1186/s12911-023-02115-5.

[6] Cara Confer Hart, Moskowitz Peter, and Sambasivam Sam. “Exploring the Experiences of Primary Care Staff Due to the Lack of Interoperability between Electronic Health Records”. AAI29166138. PhD thesis. 2022. ISBN: 9798426831438.

[7] Ava Hajian, Victor R. Prybutok, and Hsia-Ching Chang. “An empirical study for blockchain-based information sharing systems in electronic health records: A mediation perspective”. In: *Computers in Human Behavior* 138 (2023), p. 107471. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2022.107471. URL: https://www.sciencedirect.com/science/article/pii/S0747563222002916.

[8] Jan Piasecki and Phaik Cheah. “Ownership of individual-level health data, data sharing, and data governance”. In: *BMC Medical Ethics* 23 (Oct. 2022). DOI: 10.1186/s12910-022-00848-y.

[9] Alex Roehrs, Cristiano André da Costa, and Rodrigo Righi. “OmniPHR: A Distributed Architecture Model to Integrate Personal Health Records”. In: *Journal of Biomedical Informatics* 71 (May 2017). DOI: 10.1016/j.jbi.2017.05.012.

[10] Asaph Azaria et al. “MedRec: Using Blockchain for Medical Data Access and Permission Management”. In: *2016 2nd International Conference on Open and Big Data (OBD)*. 2016, pp. 25–30. DOI: 10.1109/OBD.2016.11.

[11] Xueping Liang et al. “Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications”. In: Oct. 2017. DOI: 10.1109/PIMRC.2017.8292361.

[12] Gaby G. Dagher et al. “Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology”. In: *Sustainable Cities and Society* 39 (2018), pp. 283–297. ISSN: 2210-6707. DOI: https://doi.org/10.1016/j.scs.2018.02.014. URL: https://www.sciencedirect.com/science/article/pii/S2210670717310685.

[13] Shivansh Kumar, Aman Bharti, and Ruhul Amin. “Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions”. In: *Security and Privacy* 4 (Apr. 2021). DOI: 10.1002/spy2.162.

[14] Alixandra Taylor et al. “VigilRx: A Scalable and Interoperable Prescription Management System Using Blockchain”. In: *IEEE Access* 10 (2022), pp. 25973–25986. DOI: 10.1109/ACCESS.2022.3156015.

[15] Kebira Azbeg, Ouaïl Ouchetto, and Said jai andaloussi. “BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security”. In: *Egyptian Informatics Journal* 23 (Feb. 2022). DOI: 10.1016/j.eij.2022.02.004.

[16] Md. Ariful Islam et al. “Distributed Ledger Technology Based Integrated Healthcare Solution for Bangladesh”. In: *IEEE Access* 11 (2023), pp. 51527–51556. DOI: 10.1109/ACCESS.2023.3279724.

[17] Tejaswini S. Sawant et al. “Decentralized EHR Storage Using Blockchain”. In: *ECS Transactions* (2022). URL: https://api.semanticscholar.org/CorpusID:248461154.

[18] Hairong Lv Qingzhu Yang Qiao Liu. “A Decentralized System for Medical Data Management via Blockchain”. In: *Journal of Internet Technology* 21 (Sept. 2020), pp. 1335–1345.

[19] Vinay Chamola et al. “Artificial Intelligence Assisted Blockchain-based Framework for Smart and Secure EMR Management”. In: *Neural Computing and Applications* 35 (Mar. 2022). DOI: 10.1007/s00521-022-07087-7.

[20] Mohsan. “Decentralized Patient-Centric Report and Medical Image Management System Based on Blockchain Technology and the Inter-Planetary File System”. In: *International journal of environmental research and public health* 19(22) (Nov. 2022). DOI: 10.3390/ijerph192214641.

[21] Hyperledger Foundation. *Hyperledger Besu*. URL: https://www.hyperledger.org/use/besu.

[22] Hyperledger Foundation. *The Hyperledger FireFly Story: Kaleido Taps into the Hyperledger Community to Develop Next-Gen Solutions*. URL: https://www.hyperledger.org/case-studies/kaleido-case-study.

[23] Hyperledger Firefly Introduction. *Introduction to Hyperledger FireFly*. URL: https://hyperledger.github.io/firefly/v1.2.0/overview/supernode_concept.html.

[24] InterPlanetary File System. *What is IPFS*. URL: https://docs.ipfs.tech/concepts/what-is-ipfs/?fbclid=IwAR2ac1HfOKxPc8hltlf0nxSdsfQK8PMZsn_Xe4B4B-kgndT%20zP3YdRIp7Tsw.

[25] Hospital Services Management - DGHS. *Specialized hospitals list*. 2019. URL: http://hospitaldghs.gov.bd/wp-content/uploads/2019/12/Specialized-hospital.pdf.

[26] Hyperledger Foundations. *Create a custom identity, Hyperledger Firefly*. URL: https://hyperledger.github.io/firefly/v1.2.0/tutorials/create_custom_identity.html.

[27] Hyperledger BESU. *Proof of authority consensus*. URL: https://besu.hyperledger.org/private-networks/concepts/poa.

[28] ScienceDirect. *Byzantine fault detection*. URL: https://www.sciencedirect.com/topics/computer-science/byzantine-fault.