Blockchain-based Secure Healthcare System: A Testcase of Hyperledger Fabric for Medical Data Management

Mallika Dey and Al Imran
Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka-1342
Correspondence E-mail: mallikaju307@gmail.com

***Abstract*—In recent years, the healthcare industry has experienced significant growth in the amount of sensitive information that is being exchanged and stored digitally. This has created new challenges for healthcare organizations in terms of safeguarding patient data from security threats and unauthorized access. Blockchain technology has emerged as a promising solution to address these challenges. This paper proposes a blockchain-based secure healthcare system using Hyperledger Fabric. This system employs smart contracts to manage medical data and access control.**

***Index Terms*— Blockchain, Hyperledger Fabric, Electronic health record, Chaincode and Wallet.**

I. Introduction

The healthcare system aims to promote and maintain the well-being of individuals. It covers prevention, diagnosis, treatment, and rehabilitation, as well as a range of medical specialists, facilities, and technologies. Efficient management of healthcare services is crucial to ensuring high-quality care and improving patient health outcomes. The term medical data comes with digital healthcare. Medical data is an important component of digital healthcare. Medical data may include patient health records, medical im ages, diagnostic test results, etc. Since medical data contains sensitive information, ensuring the securityof medical data is important. The healthcare industry faces various challenges regarding the secure storage and management of medical data. There is a growing need for a secure and transparent system for storing, accessing, and sharing medical records between patients, doctors, and hospitals. Problems with traditional systems - lack of transparency and security, privacy concerns and data breaches, unable to ensure tamperproof records. In this paper, a blockchain-based healthcare system is proposed to overcome these problems.

Blockchain technology, introduced by Satoshi Nakamoto in 2008, has emerged as a revolutionary tool for addressing such challenges. Blockchain is a decentralized, immutable ledger that uses cryptography to ensure data security and transparency without relying on a central authority [1]. Once a block of data is added to the ledger, then it is extremely difficult to remove or edit. That makes blockchain different from other databases. Blockchain can be permissioned and permissionless. In a permissionless blockchain, anyone can join the network. Permissioned blockchain is only accessible to the permissioned user. Some of the permissioned blockchains are Ripple, Hyperledger Fabric, and Hyperledger Besu.[2] Hyperledger Fabric is a blockchain technology designed to build applications with a modular architecture. It is an open-source permissioned DLT (Distributed Ledger Technology) platform from the Linux Foundation. It was designed for the enterprise. It supports Java, Go, and Node.js programming languages. Modular components of Fabric are the configuration of the ledger to support DBMS, pluggable membership service provider for private data management [3]. It allows developersto modify membership services and consensus algorithms [4]. The implementation of blockchain in healthcare has demonstrated significant outcomes. Blockchain-based systems provide secure electronic health records (EHRs) that ensure data integrity and patient privacy [5]. Additionally, they facilitate interoperability between healthcare providers, enhancing care coordination and reducing redundant medical tests [6]. Blockchain can also mitigate the risks of medical fraud and unauthorized data access by incorporating smart contracts for automated verification and access control [7]. Our contributions to this system include chaincode development for private data collection (PDC) signature verification, unique identity management, and ensuring security.

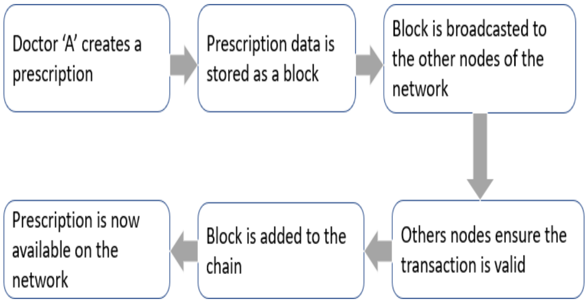

Doctor 'A' creates a prescription
Prescription data is stored as a block
Block is broadcasted to the other nodes of the network
Others nodes ensure the transaction is valid
Block is added to the chain
Prescription is now available on the network

Fig.1. Blockchain working mechanism

We have verified the signature to identify the fake prescriptions. Fig.1 shows the blockchain's working mechanism.

The system aims to provide secure storage, identity verification for patients and doctors, and traceability for medical prescriptions. Key objectives include improving data privacy, enabling secure inter-organizational sharing. This paper contains seven sections Introduction, Motivation, Literature review, Core complements, System design, Results and conclusion respectively.

II. Motivation

After facing the situation of the Covid-19 pan- demic, everyone is realizing the importance of per- sonal medical information. Patients need to know the information about their previous treatment to take the new medicine which is prescribed by an- other doctor in another healthcare organization. Butmost of the time, patients do not have their health records in an organized manner. Most healthcare organizations do not provide effective excess to patients of their data. Thus, they interact with the record in a broken manner. But we hardly recognizethis personal medical data is very sensitive for everyindividual. Hence, there is scope for misinterpretation between doctor and patient. And a single mis- interpretation of medical data can bring a massive health disaster for patients. In this circumstance, we should think about a secure and transparent system that can store personal medical data privately and protectively and which is also accessible to patients. In this case, blockchain can play an important role in solving this problem. This system aims to reduce errors in medical record keeping and tries to provide confidentiality by developing an easily accessible interface and a smart contract for interacting be- tween doctors and patients, and a smart verification system. By this, the identity of the doctors and patients can be verified.

III. LITERATURE REVIEW

A. Blockchain

The paper [1] is about the introduction toblockchain. It also stated the algorithms behind the blockchain, its applications, and technical challenges.

Structure: Blockchain is chronologically sorted. It is a continuously growing list of records known as blocks and secured using cryptography. Here, each block contains individual transactions. Each block has its own hash value and the previous block's hashvalue. However, there is no previous hash in the starting block. It is also known as the Genesis block. Blocks hold the hash of each valid transaction under this block and encodes it into a Merkle tree. Merkle tree is a binary tree. The Merkle root contains the hash of all transactions under a block. And leaves of the Merkle tree contain individual transaction hash.

The block time is the average time to create a new block in the blockchain network. Here, they discuss some of the applications of blockchain, like, data analysis and management in big data analytics and artificial intelligence with blockchain's smart contract. Paper [10] provided an overview of blockchain applications in healthcare, focusing on improving supply chain management, drug traceability, and fraud prevention.

B. Private Data Collection

The paper [3] discusses the vulnerability of private data collection and designs a feature for the Hyperledger fabric to mitigate attacks. Private data collection allows for selective data sharing among peers while keeping the data confidential from other peers in the network. 91.67% of PDC-related projects have PDC leakage problems, and 86.51% ofthem are potentially vulnerable to fake PDC results injection attacks. The authors demonstrate three categories of use case scenarios concerning endorsing, endorsement policy, and transaction semantics where misused features cause security issues. Paper [8] presented a framework for leveraging blockchain to prevent data tampering and unauthorized access in cloud-based EHR systems.

C. Medical Data

Medical data is a collection of records of a patient's health history, which is prescribed by any doctor of any healthcare company. When a patient would likely to switch to another doctorfor visiting, he needs his previous medical record. Still, most of the previous records are maintained by the previous healthcare organization, which is not accessible to the patient. In this case, a lack of proper documentation of previous medical records may lead to misinterpretation. Here blockchain can play a vital role in accessing and storing medical data in an organized manner [4]. The world is moving towards electronic medical records (EMR) management systems to protect personal medical information. An EMR contains a patient's medical history, including reports of previous medical tests and therapies, as well as names of medications prescribed by the doctor [5]. A blockchain-based EMR system can be considered a protocol that enables users to store and access their medical records while ensuring privacy and security. The system has numerous advantages, including the following - There is no centralized owner or hubfor a hacker to corrupt or infiltrate; records are updated and available at all times, and data from various sources is combined into a database thatis public and easily verifiable among non-affiliated provider organizations. In the paper [6], the authors discuss the process of securing medical information through the Hyperledger blockchain and also propose a deep-learning diagnosis model. Their proposed modelis HBESDM-DLD. This model has several phases of security systems, like encryption andoptimal key generation. Their idea was to encrypthealth records using SIMON block cipher alongwith a GTOA-based key generation technique. Legal users will be able to decrypt cipher data.To determine the existence of diseases, variationalautoencoder-based diagnostics will be performed. Electronic health records offer chances to improvepatient care, incorporate performance metrics into clinical practice, and allow clinical research [7]. Paper [9] explored the integration of blockchain with advanced encryption techniques to create a secure and scalable system for clinical data exchange. EHRs typically incorporate data on demographics, vital statistics, administration, claims (medical and pharmacy), clinical, and patient-centered topics (such as information gleaned through frailty or caregiver assessments, home monitoring devices, or health-related quality-of-life instruments).

IV. CORE COMPONENTS

The core components of the Hyperledger Fabric include the certificate authority (CA), channel, chaincode, wallets, and state database.

A. *Certificate Authority*

The CA generates a private and public key to issue identities. Mainly, CA services deal with user registration, blockchain transactions, and TLS- secured interactions between users or blockchain components.

B. *Channel*

Channel is a subnet of the network and isolates the smart contract and the state. All peers belongingto the same channel have access to the same smart contract and the data. Any outsider cannot access the ledger in the channel.

C. *Chaincode*

Smart contracts are packaged into a chaincode and then deployed to the blockchain. Chaincodehandles business logic and manages the ledger state.

D. *Wallets*

A Wallet contains the identities. A user can connect to a channel and make a transaction using these identities.

E. *World State Databases*

Hyperledger Fabric provides the facility to view the current state of the blockchain in CouchDB and LevelDB. LevelDB is the default state database. But one can use CouchDB. It stores data in JSON formatand issues rich queries.

V. System design

The system is developed based on private data collection. There is only one channel in this sys- tem. Fig.2 shows the technical architecture of this blockchain-based healthcare system with two channels.

Channel Config (CC) - Defines network policies, peers, organizations, and ordering nodes. Orderer(O) - The orderer peer chronologically sortsthe transactions and creates blocks [3]. Peer(P) - In Hyperledger Fabric, a peer is a type of node that executes consensus protocol to validate transactions. Types of peers - endorser peer, committer peer. The endorser peer endorses a transaction, and the committer peer updates the ledger. Smart contract(S) - Defines transaction logic. Ledger(L) - Consists of world state and blockchain. Each organization in the network has its own CA, which issues and manages digital certificates for network participants. Three actors are considered in the system- admin, patient, and doctor. The following Fig.3 depicts the sequence diagram for creating a prescription. The doctor sends a request to the system to generate a prescription. Fabric- sdk generates a signature using the ECDSA with SHA256 algorithm for the prescription. Then fabric- sdk will verify the doctor and determine permissions using the X.509 certificate. When the doctor’sidentity is verified, fabric-sdk will send a request to peers to create a transaction. Here, Fabric Soft- ware Development Kit (SDK) interacts with the Hyperledger Fabric network. It provides the APIs that allow seamless integration between the front- end application and the blockchain network. The authenticity of the prescriptions was verified using the digital signature of the doctor who created the prescription. The signature was generated using the doctor’s private key and can be verified using the doctor’s public key, which is available in the CA. We break down the signature verification process into several steps, as depicted in Fig. 4.

First, we fetch a block of a particular transaction id anduse BlockDecoder to parse and decode the block.Data in the blockchain is stored in buffer format.We need to work with the protocol buffer message returned by GetBlockByTxID to verify a signature. Here, the envelope contains the signature header & the payload. The signature header contains the signcreated by the user’s private key.

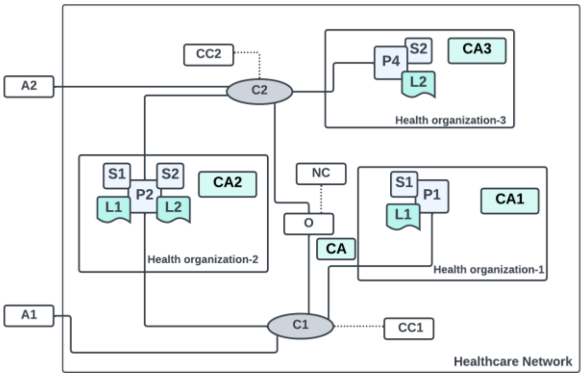


Fig. 2: Technical Architecture

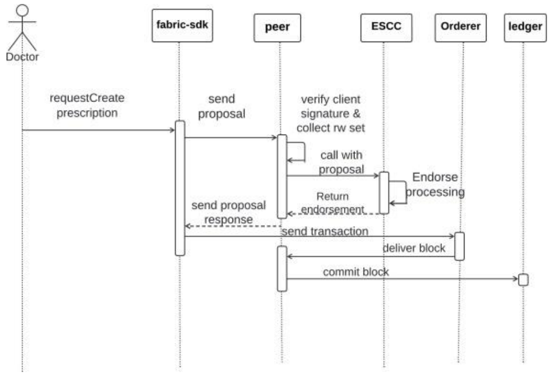


Fig. 3: Sequence diagram for creating prescription

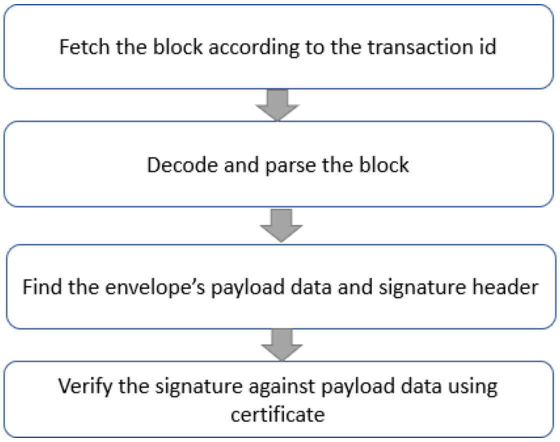

Fetch the block according to the transaction id
Decode and parse the block
Find the envelope’s payload data and signature header
Verify the signature against payload data using certificate

Fig. 4: Signature verification

The signature can be verified against those serialized payload bytes. The sequence diagram in Fig.5 illustrates the sequence of interactions involved in the signature verification process. The doctor will send a request to Fabric-sdk for signature verification. Fabric-sdk will fetch the block using the transaction id of the prescription. The peer will find the block from theledger and send it to fabric-sdk. Fabric-sdk willextract the block, verify the signature, and then sendthe result to the patient. If the peer fails to fetch the block, it will send an invalid response to fabric-sdk.

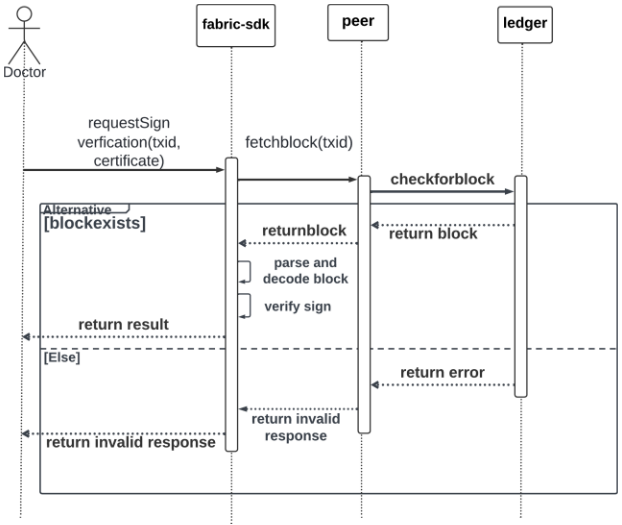


Fig. 5: Sequence diagram of signature verification

Fig.6 shows the private data model used by health organizations for private data collection. Private data is kept off-chain and available only to a subset of organizations in the channel. Here in this model, prescribed medicine is kept secret.

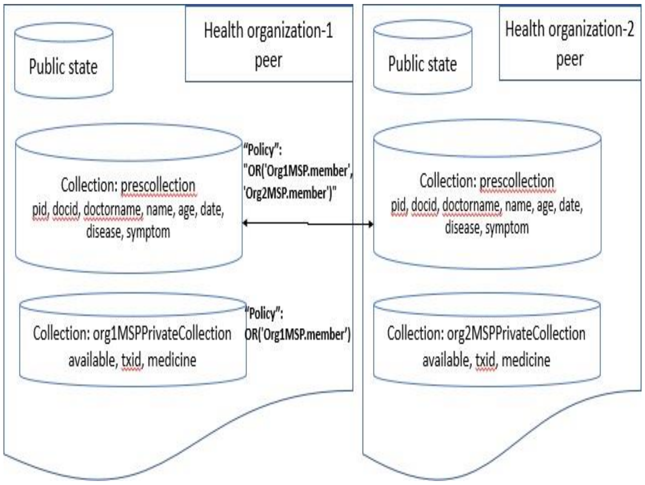

Public state
Health organization-1 peer
Collection: prescollection
pid, docid, doctorname, name, age, date, disease, symptom
"Policy": "OR('Org1MSP.member', 'Org2MSP.member')"
Collection: org1MSPPrivateCollection
available, txid, medicine
"Policy": OR('Org1MSP.member')
Public state
Health organization-2 peer
Collection: prescollection
pid, docid, doctorname, name, age, date, disease, symptom
Collection: org2MSPPrivateCollection
available, txid, medicine

Fig. 6: Private data model

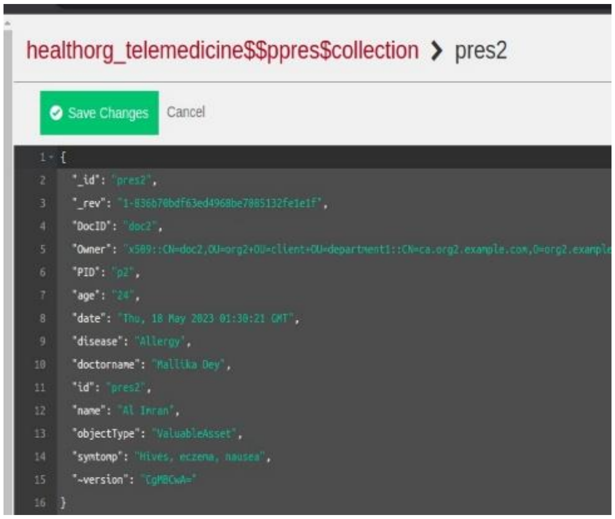
VI. RESULT AND DISCUSSION

We have used CouchDB as the state database in this system. Here, a prescription with the id "pres2" is generated by the doctor affiliated with organization-2. Fig.7 shows the public data of the prescription. Fig.8 shows the private data of theprescription. Members of organization-2 can share these private data with other organizations in the network.

A. Performance evaluation

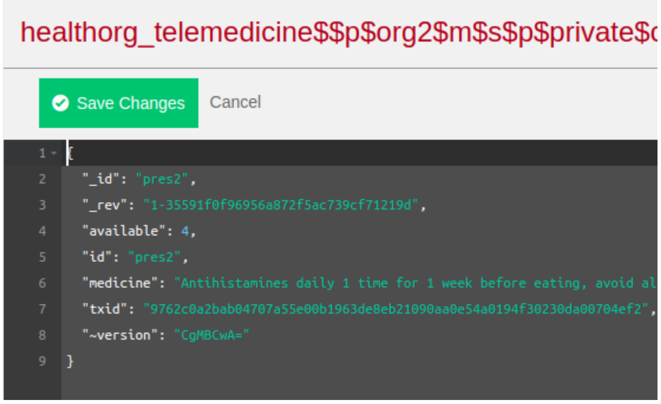
The system was tested on a Linux machine with 16GB RAM and a 20GB hard disk. The following results were observed:
Transaction Throughput: The system processed 7200 transactions (986.1 KB) in approximately 5 hours**.**

Scalability: The modular architecture supports horizontal scaling by adding more nodes**.**



```
{
  "_id": "pres2",
  "_rev": "1-836b70bdf63ed4968be7885132fe1e1f",
  "DocID": "doc2",
  "Owner": "x509::CN=doc2,OU=org2+OU=client+OU=department1::CN=ca.org2.example.com,O=org2.example
  "PID": "p2",
  "age": "24",
  "date": "Thu, 18 May 2023 01:30:21 GMT",
  "disease": "Allergy",
  "doctorname": "Mallika Dey",
  "id": "pres2",
  "name": "Al Imran",
  "objectType": "ValuableAsset",
  "symtomp": "Hives, eczema, nausea",
  "~version": "CgMBCwA="
}
```

Fig. 7: Public details

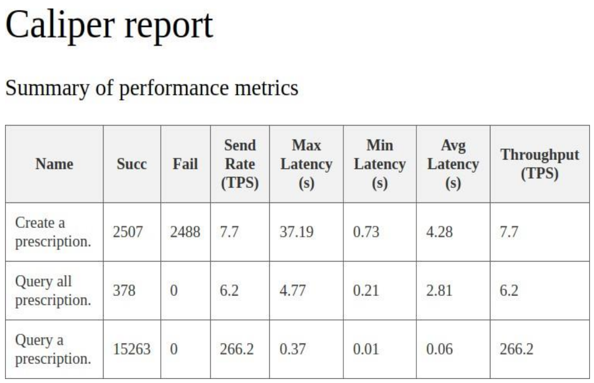


```
{
  "_id": "pres2",
  "_rev": "1-35591f0f96956a872f5ac739cf71219d",
  "available": 4,
  "id": "pres2",
  "medicine": "Antihistamines daily 1 time for 1 week before eating, avoid al
  "txid": "9762c0a2bab04707a55e00b1963de8eb21090aa0e54a0194f30230da00704ef2",
  "~version": "CgMBCwA="
}
```

Fig. 8: Private details

Security: The use of Hyperledger Fabric's private data collections ensured data confidentiality.

Using Hyperledger Caliper, we conducted sys- tem benchmarking. Hyperledger Caliper is a performance benchmark tool for multiple blockchain platforms. Performance metrics of the system are transaction throughput and latency.



Caliper report

Summary of performance metrics

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
Create a prescription.	2507	2488	7.7	37.19	0.73	4.28	7.7
Query all prescription.	378	0	6.2	4.77	0.21	2.81	6.2
Query a prescription.	15263	0	266.2	0.37	0.01	0.06	266.2

Fig. 9: Throughput benchmarking

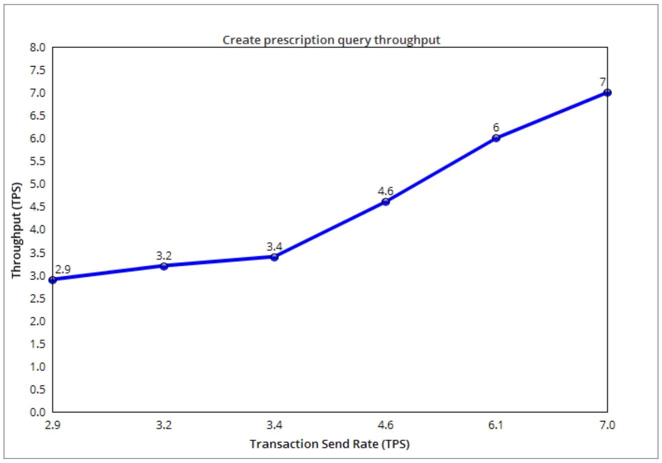


Fig. 10: Throughput (Transaction load-5)

On the other hand, Fig. 11 depicts the relationship between send rate and latency for creating prescriptions.

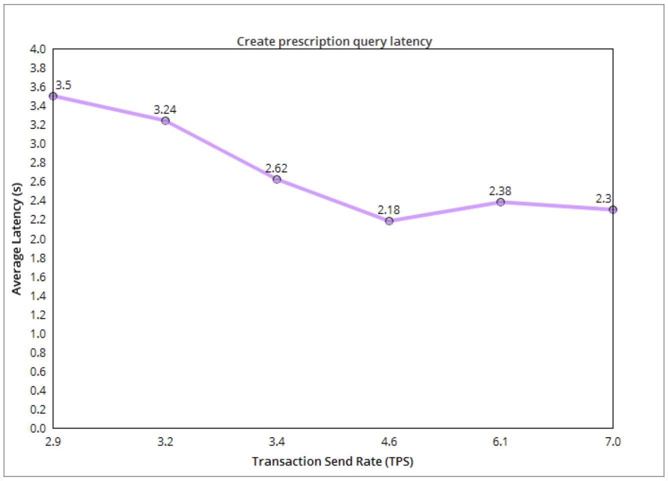


Fig. 11: Average Latency (Transaction load-5)

In Fig.11, as the send rate increases, the latency generally decreases. Fig.12 provides an overview of throughput along with the send rate of the transactions. In Fig.10, the transaction load is set to 5, while in Fig.12, the transaction load is increased to 15. In both cases, the throughput positively correlates with the send rate, indicating an upward trend. This indicates that the system can process a higher number of transactions per second as the workload intensifies.

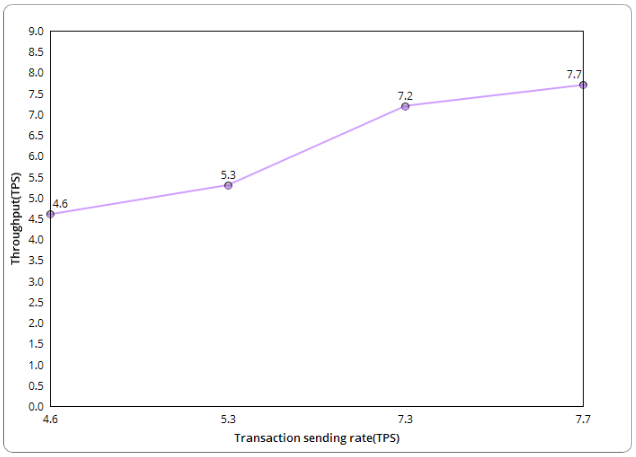


Fig. 12: Throughput (Transaction load-15)

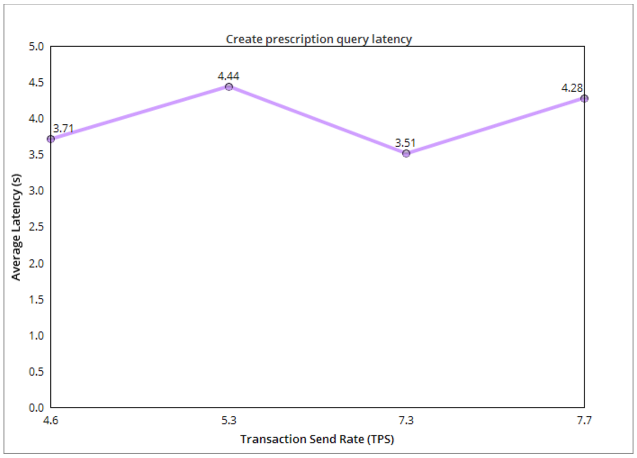


Fig. 13: Average Latency (Transaction load-15)

Fig. 13 presents the average latency associated with querying all prescriptions for a transaction load of 15. In this context, as the transaction send rate increases to 7.3, there is a noticeable decrease in average latency.

Several factors, including network configuration, hardware resources, transaction complexity, and system optimization, can influence the achieved throughput. The following graph, Fig.14, illustrates the relationship between the average latency and the send rate for prescription queries, providing valuable insights into how the system's response time varies with different transaction rates. In Fig.14, as the send rate of transactions increases, the system exhibits a significant decrease in latency.

Table I highlights the distinguishing features and characteristics of the system in contrast to other systems. It provides a comprehensive overview of the unique aspects and points of differentiation that set this system apart from its counterparts.

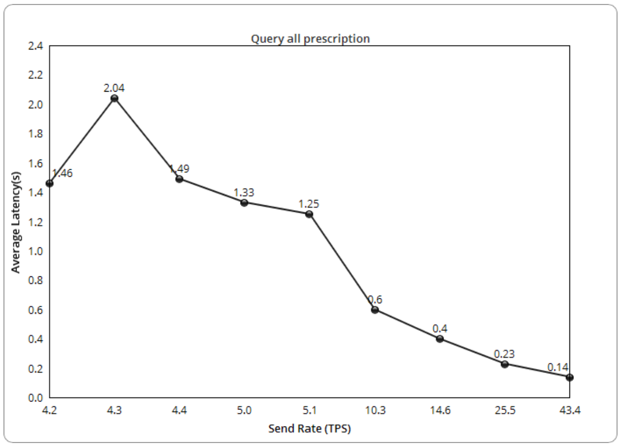


Fig. 14: Average latency for querying all prescriptions

TABLE I
Comparison Table

System Aspects	Public Blockchainbased Healthcare System	Healthcare System Using Hyperledger Fabric	Digital Other Healthcare System
Confidential	No	Yes	Perhaps
Tamper-proof	Yes	Yes	Perhaps
Computational Power	High	Low	N/A
Transparency	Yes	Yes	No
Ensuring Security	Yes	Yes	Perhaps

VII. Conclusion

By leveraging blockchain technology, we have achieved tamperproof prescription records, ensuring the integrity and immutability of medical data. Smart contracts have facilitated automated verification and validation processes, reducing reliance on manual and error-prone procedures. The transparency offered by the blockchain has enhanced trust and accountability within the healthcare ecosystem. Since Hyperledger Fabric uses its identity verification system, a user without an identity cannot change the blockchain. In this system, data is secured as all participants are known. Through private data collection, healthcare providers gain control over sensitive patient information. This approach preserves patient privacy while allowing trusted parties to access relevant data for optimal care.

Future work: We will try to expand the network to incorporate additional organizations and enhance scalability through multi-channel architecture. Finally, we want to develop a more user-friendly interface.

Acknowledgment

We would like to express our heartfelt gratitude to Dr. Mohammad Zahidur Rahman, Professor, Department of Computer Science and Engineering, for providing valuable guidance and help.

References

[1] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[2] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis,A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, “Hyperledger fabric: a distributed operating system for permissioned blockchains,” in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[3] S. Wang, M. Yang, Y. Zhang, Y. Luo, T. Ge, X. Fu, and W. Zhao, “On private data collection of hyperledger fabric,” in *2021 IEEE 41st International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2021, pp. 819–829.

[4] D. A. Adeogun, E. O. Ogunseye, and S. O. Akinola, “Man- agement of medical data access using blockchain technology,” *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 18, no. 12, 2020.

[5] Y. Han, Y. Zhang, and S. H. Vermund, “Blockchain technology for electronic health records,” *International Journal of Environ- mental Research and Public Health*, vol. 19, no. 23, p. 15577, 2022.

[6] N. Sammeta and L. Parthiban, “Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model,” *Complex & Intelligent Systems*, vol. 8, no. 1, pp. 625–640, 2022.

[7] M. R. Cowie, J. I. Blomster, L. H. Curtis, S. Duclaux, I. Ford,F. Fritz, S. Goldman, S. Janmohamed, J. Kreuzer, M. Leenay *et al.*, “Electronic health records to facilitate clinical research,” *Clinical Research in Cardiology*, vol. 106, pp. 1–9, 2017.

[8] Xia, Q., Sifah, E. B., Asamoah, K. O., Gao, J., Du, X., & Guizani, M. (2017). "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, 5, 14757-14767.

[9] Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2018). "Secure and Trustable Electronic Medical Records Sharing using Blockchain," *AMIA Annual Symposium Proceedings*.

[10] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" *IEEE Cloud Computing*, 5(1), 31-37