MethodsX 13 (2024) 103002

Contents lists available at ScienceDirect

MethodsX

journal homepage: www.elsevier.com/locate/methodsx

A secure interoperable method for electronic health records exchange on cross platform blockchain network

Rahul Ganpatrao Sonkamble[a,b], Anupkumar M. Bongale[c,*], Shraddha Phansalkar[d], Deepak Sudhakar Dharrao[a]

[a] *Department of Computer Science and Engineering, Symbiosis Institute of Technology, Pune Campus, Symbiosis International (Deemed University), Lavale, Pune, Maharashtra 412115, India*
[b] *Pimpri Chinchwad University, Pune, Maharshtra 412106, India*
[c] *Department of Artificial Intelligence and Machine Learning, Pune Campus, Symbiosis International (Deemed University), Symbiosis Institute of Technology, Lavale, Pune, Maharashtra 412115, India*
[d] *Computer Engineering, MIT Art, Design and Technology University, Pune, Maharashtra 412201, India*

ARTICLE INFO

Method name:
A method for secure EHR exchange on Ethereum and Hyperledger fabric network

Keywords:
Electronic health records
Interplanetary file systems
Blockchain
Ethereum
Hyperledger fabric
Interoperability
Cross-chain
Secure password authentication-based key exchange

ABSTRACT

An Electronic Health Record (EHR) store essential and sensitive patient's medical information. Since health information is highly confidential data, it should be accessible with the consent of the patient. Blockchain based EHR management system offers improvised privacy and patient-centric approach. EHR management systems are available with multiple blockchain platforms. Generally, EHRs are maintained at several independent blockchain platforms. EHR management systems should be capable of securely exchange data on cross platform blockchain network. The interoperability in such blockchain platforms should facilitate seamless cross-chain interaction and information exchange. This article proposes a method that facilitates secure EHR exchange on Ethereum and Hyperledger fabric network using hepatitis dataset. The key contributions of the proposed method include:

- Hash lock based interoperable cross-chain method for EHR exchange across Ethereum and Hyperledger fabric.
- Additional security to the EHR is ensured by partitioning EHR as on-chain (blockchain platform) and off-chain InterPlanetary File System (IPFS)
- Secure Password Authentication-Based Key Exchange (SPAKE) based session management for EHR exchange across two parties.

The proposed patient centric method is validated to ensures the successful exchange of patient EHR across Ethereum and Hyperledger fabric.

Specifications table

Subject area:	Computer Science
More specific subject area:	*Blockchain*
Name of your method:	*A method for secure EHR exchange on Ethereum and Hyperledger fabric network*
Name and reference of original method:	*NA*
Resource availability:	*Hepatitis dataset used in this research is available at* https://archive.ics.uci.edu/dataset/46/hepatitis *under Creative Commons Attribution 4.0 International (CC BY 4.0) license*

* Corresponding author.
E-mail address: anupkumar.bongale@sitpune.edu.in (A.M. Bongale).

https://doi.org/10.1016/j.mex.2024.103002
Received 9 August 2024; Accepted 8 October 2024
Available online 10 October 2024
2215-0161/© 2024 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

Background

Interoperability is a pivotal concept within the realm of blockchain technology [1]. It denotes the capacity of distinct blockchain systems or networks to interact and share information with one another. This capacity of distinct blockchain networks to seamlessly communicate and collaborate [2,3]. This analogy likens blockchains to unique islands, each with its distinct rules, languages, and currencies [4]. This concept holds great significance due to the extensive diversity within the blockchain ecosystem, featuring various blockchains tailored to specific purposes and industries [5]. Notably, Bitcoin, Ethereum, and other blockchains possess their unique strengths and weaknesses but frequently operate in isolated silos. Interoperability seeks to dismantle these isolation barriers, fostering cooperation among divergent blockchain systems [6]. In the context of blockchain technology, interoperability assumes a crucial role in enabling secure data exchange and trust-based transactions among different blockchain systems. The concept of interoperability in blockchain technology bears similarities to the notion of network infrastructure, allowing industry partners to exchange data across a network. In the context of blockchain, interoperability signifies the ability of various blockchain systems or networks to communicate and share information effectively. Interoperability solutions adopt diverse approaches, encompassing the development of specialized protocols or middleware layers designed to translate and transmit data across blockchains [7]. Alternatively, some solutions employ atomic swaps or bridge mechanisms to facilitate secure asset transfers between different blockchain networks [8]. Such solutions empower a wide array of applications, including Decentralized Finance (DeFi) platforms that gain access to assets on various chains, crosschain asset transfers, and even the execution of multi-chain smart contracts [9]. The challenges associated with achieving interoperability in blockchain systems encompass data security and industry standards for governing and overseeing applications. Interoperability refers to the interchange of digital assets and transaction data between various blockchain and goes beyond merely facilitating communication and data exchange among diverse applications [10].

The significance of interoperability in this context can be summarized with the factors like Streamlined Asset Mobility [11,12], Cross-Platform Versatility [13,14], Enhanced Scalability and Efficiency [15], Empowering DeFi [16], Mitigating Risk [15], Cross-Chain Smart Contracts [4,17–19], Boosting Adoption [20], Global Accessibility [21], Compliance with Regulations [22,23], Future-Proofing etc. Because of the advantages of blockchain technology, it is being used healthcare domain as well. But healthcare facility may deploy different blockchain platforms. So, cross-chain for EHR transfer should be promoted. It offers a multitude of advantages and effectively addresses critical challenges in the management of healthcare data like Seamless Data Integration [24], Continuity in Patient Care [25], Empowering Patients [6], Error Reduction [26], Operational Efficiency [4,27], Fuelling Research and Innovation [28], Enhanced Security and Privacy [4,6,29], Resilience in Data Management [4], Global Health Initiatives [30], Standardization [4], Cost-Efficiency [4], Regulatory Compliance [4], Enhanced Patient Engagement [4], Telemedicine Support [31], Advancing Preventive Care [32] etc. Significance of general interoperability and with respect to healthcare is depicted in Fig. 1.

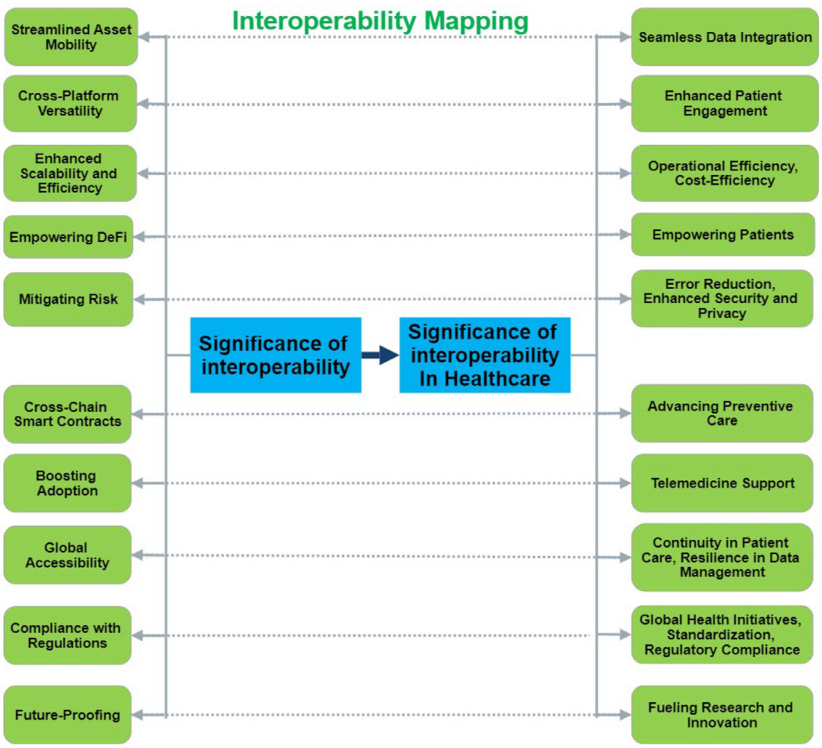

Fig. 1. Interoperability significance mapping with respect to healthcare systems.

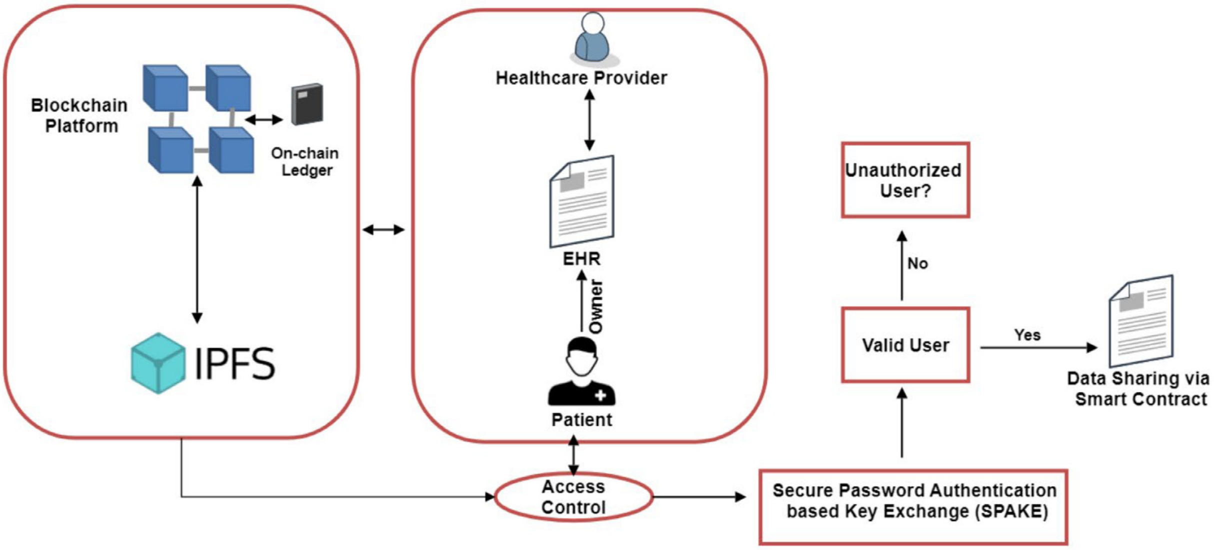

Fig. 2. Basic method for the blockchain platform based EHR access.

Method details

This section introduces components used for cross-chain interoperability based on hash locking. The proposed method is developed for secure EHR exchange on Ethereum and Hyperledger fabric network for the management of patient medical records. Based on the application domain demands, a different blockchain network's platform determines the relevant properties. Apart from EHR exchange, the interoperable blockchain methods have several applications such as cross-chain tokenized trading assets and supply chain management. Trading assets can be exchanged across the Ethereum and Hyperledger with hash lock-based mechanism to provide the trust enabled cross-chain trading. Similarly, the sensitive data such as supplier information, product process, and cost details can be handled on a private network by Hyperledger fabric, and the public attributes like shipping confirmations, and product quality certifications can be handled by the public Ethereum blockchain.

Basic method for EHR storage and accessibility

The basic component of blockchain platform based EHR access is as shown in Fig. 2. This method is used for our cross-chain EHR transfer. Only an authenticated patient or healthcare stakeholder will be able to access EHR. Authentication will be done by the Secure Password Authentication-Based Key Exchange (SPAKE) protocol. SPAKE protocols are cryptographic methods designed to establish a secure session key between two parties using a shared password, enhancing security in authorization systems [28,33]. SPAKE safeguards against offline dictionary attacks by deriving cryptographic keys from passwords, making it challenging for attackers to discover the original password.

After storing EHR, it is partitioned into on-chain and off-chain process [34,35]. Such EHR partitioning is required to preserve the privacy. Only the identity attributes of the patient will be stored on-chain. Remaining medical information like reports will be stored off-chain. As the identity attributes are separated from the main health record, it will be difficult to identify the patient to whom the EHR belongs. Hash of identity attributes can be mapped with off-chain id to retrieve the record using the smart contract. With such partitioning we can maintain anonymity and disassociation to preserve the privacy. We have used InterPlanetary File System (IPFS) for the off-chain. IPFS is a distributed file system which connects the communicating devices for the same system of files [36,37]. EHR partitioning is important to minimize the access cost and storage cost apart from maintaining the privacy. Other components of this architecture are as follows.

Off-chain storage

IPFS [38] is a unique protocol and peer-to-peer network designed for storing and sharing data within a distributed file system. It employs content-addressing, a method that assigns a unique cryptographic hash to each file, creating a global namespace that links IPFS hosts. IPFS serves as both a protocol and a network, introducing an innovative approach to web development. It empowers users to access and share data via a decentralized network. IPFS relies on content-based addressing, where files are identified by their distinct cryptographic hash based on their content. This approach guarantees data integrity and facilitates efficient retrieval. This research proposes the system with consideration of Ethereum [39] and Hyperledger fabric [40] as blockchain platforms.

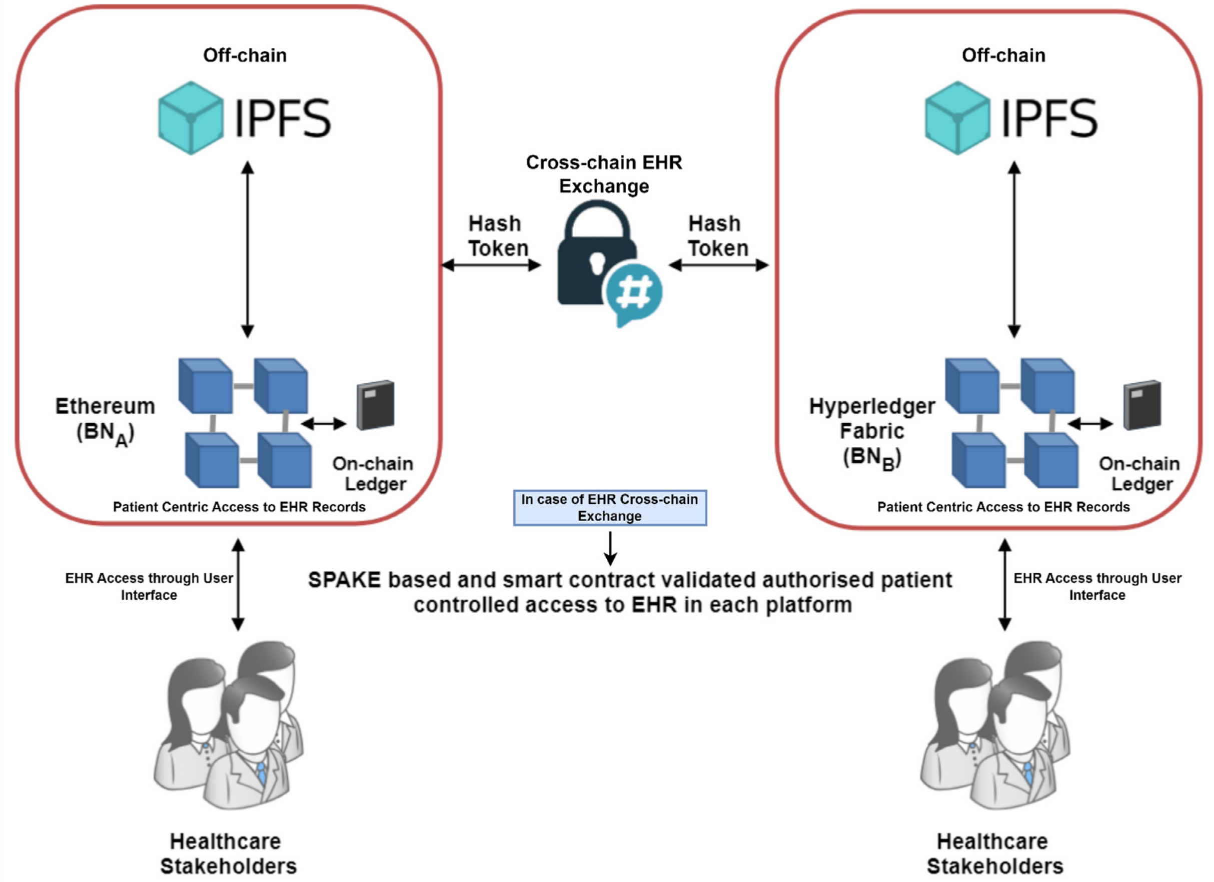

Fig. 3. Hash lock-based cross-chain interaction method.

Blockchain platforms

Ethereum [39] offers implementation of logic through programming in blockchain ledger in addition to the primary blockchain ledger through smart contracts usage. To run smart contract code and transfer assets via tokens gas is required, using Ether cryptocurrency. Gas is paid in wei units, where 1 Ether = 10^{18} Wei. When the transaction of a smart contract is carried out, certain gas units are needed for computation. These gas units are then transformed into Gwei units depending on the gas price.

Fabric stands out as a prominent permissioned blockchain framework, nestled within the Linux Foundation's expansive Hyperledger consortium [40]. Tailored specifically for enterprise applications, Fabric champions permissioned participation, ideal for scenarios where network members are well-known and trusted, such as business consortia. Fabric extends support to smart contracts authored in popular programming languages like Go and Node.js, simplifying development and accessibility for programmers. Notably, Fabric excels in preserving privacy, facilitating confidential transactions among specific participants while preserving network integrity. A multitude of organizations, including industry giants like IBM, harness the capabilities of Fabric to construct blockchain solutions across a spectrum of sectors, spanning finance, healthcare [41,42], and supply chain management [42]. So, considering the system architecture as shown in Fig. 2 for ethereum and hyperledger fabric will be as shown in Fig. 3.

Hash-locking operates on the same premise as lightning networks'Hash-Time-Locking (HTLC). It is a tool that lets users make educated guesses about the hash value's initial value for a specified period. The related assets are locked when someone sends them to someone else by sending the hash value of the asset to the recipient. The locked asset will be transferred to the receiver if they can determine the hash value of the locked cryptocurrency correctly. Some improved HTLC-based procedures have been established as a result of the high communication, high payment cost, and low-efficiency overhead of HTLC.

The sequence of interactions

Whenever cross-chain EHR transfer is initiated then there are few interactions among the blockchain networks through the hash lock mechanism as shown in Fig. 4. Notations of BN_A for Ethereum and BN_B for Hyperledger Fabric are used in this article. The following use case scenario is represented with the assumption that doctor of BN_A is requesting EHR from BN_A. Patient identity

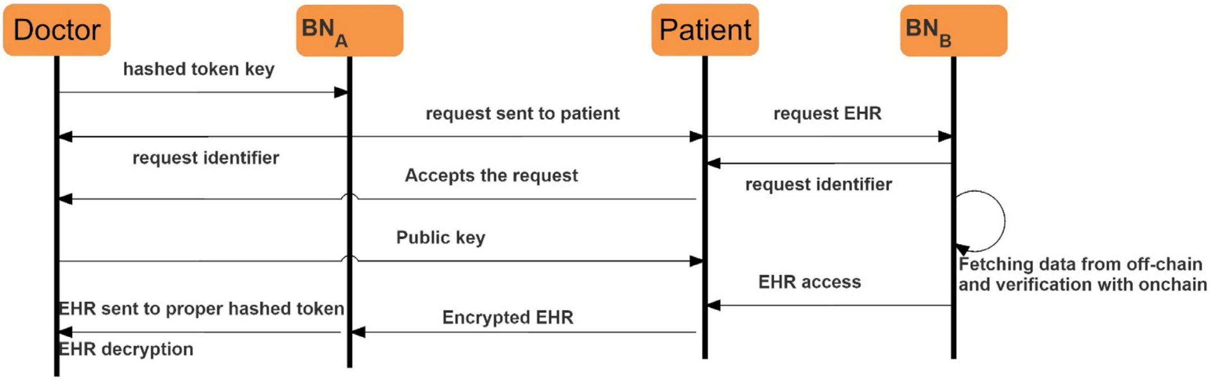

Fig. 4. Cross-chain interaction communication Sequence.

attributes i.e. Patient ID, Patient name are stored on the blockchain ledger and remaining health information is stored on off-chain storage i.e. at IPFS. Assumption is that BN_A & BN_B have their consensus verifiers registered together with the doctor and the patient. With these considerations the following steps give idea about the working of the system.

Step 1: The doctor is supposed to create a token and which will be used to send queries to BN_A that includes the hash of token key. The doctor provides patient the token key along with the request identification in off-chain mode that the network provides as an event. This key and identification will be used for future use.

Step 2: Patient agrees to the request generated by doctor. As that request does not include patient's identity, the patient includes the token key to the initial request. BN_A broadcasts the identity of the doctor who submitted the request to its consensus verifiers.

Step 3: Patient requests the EHR document to BN_B for the use of doctor. Consensus verifiers of BN_B are informed for fetching identity by the broadcasted patient identity request.

Step 4: With the patient's request to the BN_B, BN_B requests the identifier of the doctor through the patient in encrypted way. After receiving the patient's encrypted response, the doctor off-chains his public key for the EHR access.

Step 5: The EHR document is retrieved by BN_B verifiers from the EHR storage, and they provide BN_B with required health data. The hash of the EHR is securely kept on-chain and is confirmed by the network. The hash of the EHR is verified with the patient identity attributes from on-chain and mapped off-chain health data. Then the patient and verifier will receive tokens generated from the network.

Step 6: EHR verification of BN_B is broadcasted from the consensus verifiers of BN_A. After sufficient responses from the verifiers, BN_A delivers tokens to the patient. In this stage, the patient proceeds for the off-chain contact with the consensus verifiers to transfer the token from the BN_B verifiers to the BN_A verifiers. New encryption is generated by patient for the encrypted scenario and provides it to the BN_B as well. It uses doctor's private and public keys for that.

Step 7: A link is established between the two verifiers so that the EHR document can be sent from BN_B to BN_A. In the encrypted scenario, the verifier uses the re-encryption key. Using this key state of the EHR is changed from the patient to the doctor once the transmission of the EHR is complete.

***Step 8*:** The BN_A verifier informs its network that the document and supporting evidence are available. For the EHR document's final transfer, the network subsequently delivers tokens to the doctor and verifiers.

Step 9: After connection establishment between doctor and verifier using their unique tokens, the doctor receives the EHR from the verifier. The private key of the doctor is used for decryption of EHR.

Method validation

Hepatitis is a significant worldwide health issue. It affected millions of people throughout the world. The research work presented in this article use hepatitis dataset [43]. Hepatitis dataset is preferred as EHR for the validation of proposed method to ensure exchange of patient EHR across Ethereum and Hyperledger Fabric crossEHR blockchain. This dataset is a versatile multivariate data including integer, categorical, and real features. It consists of 155 instances with 19 attributes - class, age, sex, bilirubin, antivirals, liver firmness, steroids, ascites, protime, fatigue, malaise, and other relevant characteristics.

The Ethereum based EHR blockchain network tested in Sepolia test network [44] sandbox and smart contracts are deployed on Truffle ver. 5.11.5 [45]. MetaMask ver.11.11.4. a digital wallet, is used to interact with the Ethereum blockchain [46]. In similar fashion, Hyperledger Fabric blockchain network which follows enterprise level modular architecture and permissioned access, is designed for four peers (commitment nodes) and single ordering node. Additionally, Docker ver. 18.06.3, Go ver. 1.13, and Python ver. 3.9 are included in the software architecture. Hardware requirement for validating the proposed method for storing and retiring EHR records over cross-blockchain platform is mentioned in Table 1.

Table 1
Hardware configuration.

Platforms	Particulars
Integrated Development Environment	Visual studio 1.85.2
Operating System	Windows 11 Education 64-bit
Memory Requirement	12 GB of RAM
Processor	i5–8500 CPU @ 3.00GHz × 6

```
struct EHR {
    uint age;
    string sex;
    bool steroid;
    bool antivirals;
    bool fatigue;
    bool malaise;
    bool anorexia;
    bool liverBig;
    bool liverFirm;
    bool spleenPalpable;
    bool spiders;
    bool ascites;
    bool varices;
    uint bilirubin;
    uint alkPhosphate;
    uint sgot;
    uint albumin;
    uint protime;
    string status;
    string ipfsCid;
}
```

Fig. 5. Ethereum dataset structure.

Ethereum and Hyperledger Fabric blockchain platforms requires representation of EHR record is specific data structure format. The Figs. 5 and 6 describes the dataset attributes of Ethereum and Hyperledger fabric respectively.

Ethereum to hyperledger fabric patient EHR exchange validation

This section describes the further validation of the proposed Cross blockchain EHR access method. The patient records stored at Ethereum blockchain platform are accessed at Hyperledger fabric platform. Rest of the section describes detailed validation of the data storage, exchange and access on cross blockchain platforms.

Patient EHR can be accessed from Hyperledger fabric to Ethereum. The EHR is portioned as on-chain and off-chain based on the relative importance of the patient records. The data from IPFS is fetched using the Content Identifier (CID) which is generated while storing the data. The patient identity attribute i.e. *patientId* is retrieved from Ethereum ledger and remaining data is fetched from the IPFS as shown in Fig. 7.

```
type EHR struct {
    Age             uint   `json:"age"`
    Sex             string `json:"sex"`
    Steroid         bool   `json:"steroid"`
    Antivirals      bool   `json:"antivirals"`
    Fatigue         bool   `json:"fatigue"`
    Malaise         bool   `json:"malaise"`
    Anorexia        bool   `json:"anorexia"`
    LiverBig        bool   `json:"liverBig"`
    LiverFirm       bool   `json:"liverFirm"`
    SpleenPalpable  bool   `json:"spleenPalpable"`
    Spiders         bool   `json:"spiders"`
    Ascites         bool   `json:"ascites"`
    Varices         bool   `json:"varices"`
    Bilirubin       uint   `json:"bilirubin"`
    AlkPhosphate    uint   `json:"alkPhosphate"`
    SGOT            uint   `json:"sgot"`
    Albumin         uint   `json:"albumin"`
    Protime         uint   `json:"protime"`
    Status          string `json:"status"`
}
```

Fig. 6. Hyperledger dataset structure.

As per the proposed method, EHR is accessible from Ethereum to Hyperledger fabric. The sample output on the Hyperledger fabric is shown in Fig. 8. Fig. 8 shows the EHR portioning where, *patientID* was fetched from the Hyperledger and remaining data is fetched from the IPFS.

With reference to cross-chain data exchange, two types of transactions, sub-transactions and cross-chain transactions are required. Sub-transactions refer to the local transactions of the individual blockchain platform. Cross-chain transactions are the transactions that are required for data transfer from one blockchain platform to another. Cross-chain data transfer is validated using CrossRate, CrossCoflictRate, and CrossSuccessRate. CrossRate is the ratio of the number of sub-transactions to number of cross-chain transactions. Fig. 9 illustrates the impact of the CrossRate ratio on sub-transactions per second (TPS).

Fig. 9 describes cross-chain transactions influence on the total number of sub-transactions within the cross-chain blockchain system. crossRate was set with value 0 which indicates blockchain platform only executes local transactions. Then the values were increased as 0.3, 0.5, 0.8, and 1. This increment indicates increase in the cross-chain transactions.

Ethereum uses Proof of Stake (PoS) consensus where blocks are confirmed by the validators. This confirmation is slow as compared to the block confirmation in Hyperledger fabric due to network congestion. Hyperledger fabric uses Practical Byzantine Fault Tolerance (PBFT) which is comparatively fast as it is permissioned blockchain. There might be delays in transaction synchronization between Ethereum and Hyperledger fabric blockchains due to different consensus algorithms. It also causes transactions to have more time for the validation. When EHR exchange is initiated, the local transaction as well as cross-chain transactions content for the resources like computational power, bandwidth, storage etc. leading to the conflict. So, the factors like delays in transaction synchronizations, different consensus algorithms, and contentions for the shared resources affect the conflicts between local transactions and cross-chain transactions. It can be observed from the Fig. 10 that as there is increment in the cross-chain transactions, there conflict of cross-chain transactions with local transactions also increases. Fig. 10 shows that cross-chain conflicts gradually increased from 0 to nearly 100%, as well SucessRate of the execution of sub-transactions is decreasing from 100% to 40%.

```
Data uploaded to IPFS with CID: QmYwAPJzv5CZsnAzt8auVZRnBrTkaZ1t6gC5bXK4h8EQni
EHR stored on Ethereum
EHR fetched from Ethereum: {
  "patientId": "patient1",
  "ipfsCid": "QmYwAPJzv5CZsnAzt8auVZRnBrTkaZ1t6gC5bXK4h8EQni"
}
EHR data from IPFS: {
  "age": 30,
  "sex": "male",
  "steroid": true,
  "antivirals": true,
  "fatigue": false,
  "malaise": false,
  "anorexia": true,
  "liverBig": false,
  "liverFirm": false,
  "spleenPalpable": true,
  "spiders": false,
  "ascites": false,
  "varices": true,
  "bilirubin": 120,
  "alkPhosphate": 120,
  "sgot": 200,
  "albumin": 380,
  "protime": 20,
  "status": "LIVE"
}
```

Fig. 7. EHR access on Ethereum platform.

```
Data uploaded to IPFS with CID: QmYwAPJzv5CZsnAzt8auVZRnBrTkaZ1t6gC5bXK4h8EQni
Transaction has been submitted
Transaction has been evaluated, result is: {
  "patientId": "patient1",
  "ipfsCid": "QmYwAPJzv5CZsnAzt8auVZRnBrTkaZ1t6gC5bXK4h8EQni"
}
EHR data from IPFS: {
  "age": 30,
  "sex": "male",
  "steroid": true,
  "antivirals": true,
  "fatigue": false,
  "malaise": false,
  "anorexia": true,
  "liverBig": false,
  "liverFirm": false,
  "spleenPalpable": true,
  "spiders": false,
  "ascites": false,
  "varices": true,
  "bilirubin": 120,
  "alkPhosphate": 120,
  "sgot": 200,
  "albumin": 380,
  "protime": 20,
  "status": "LIVE"
}
```

Fig. 8. EHR access on Hyperledger fabric platform from Ethereum.

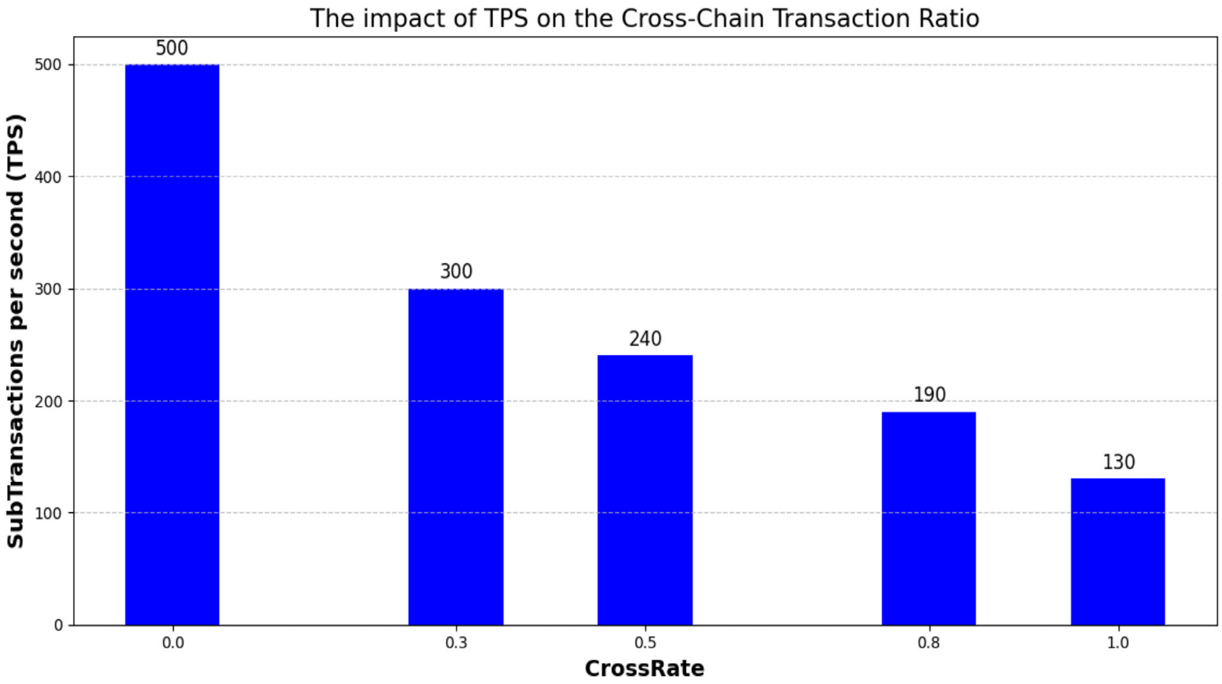

Fig. 9. Cross-chain transaction ratio effect on TPS.

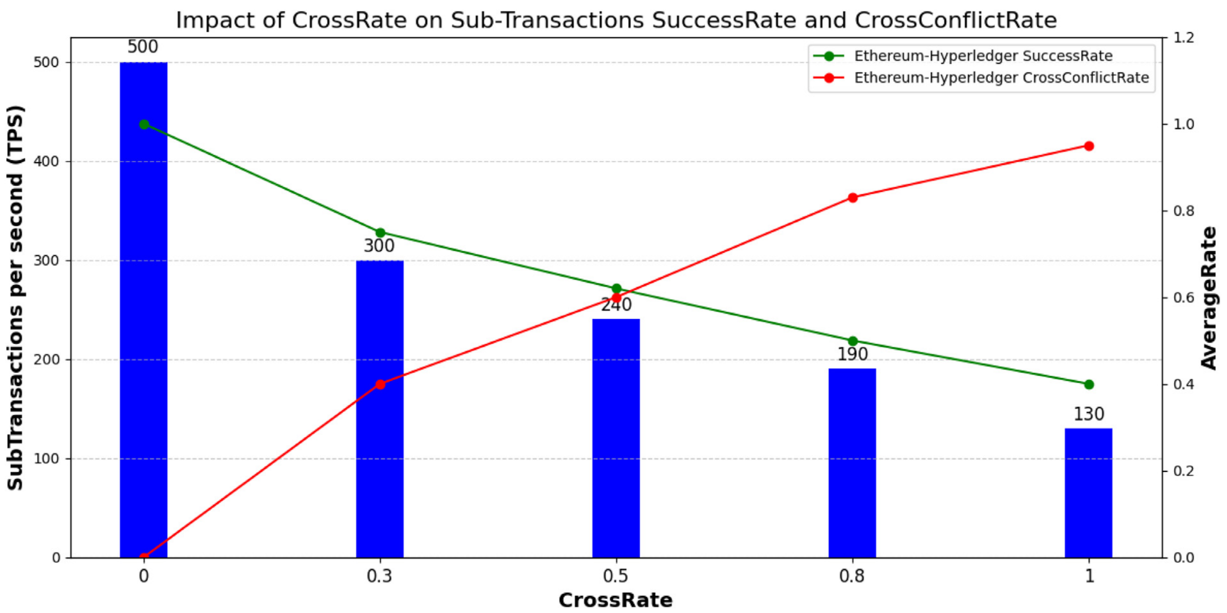

Fig. 10. Impact of CrossRate on sub-transactions successrate and crossconflictrate.

Limitations

The proposed methodology is effective enough to access the EHR cross blockchain platforms. The technology is advanced enough which includes additional scope for the future improvements. This section briefly describes the limitation of the proposed method. Scalability is still an issue especially in the peak times of the transactions in Ethereum and Hyperledger platforms. It may result in the higher gas fees and delayed transactions with added latency. Cross-conflict handling can be complex as it impacts on success of the transaction execution. In highly complex and dynamic environment, subtransaction success rates and failure rates predominantly depends on the accuracy of the systems. This can lead to network instability or smart contract bugs. Further, deployment of the cross-chain systems can be technically challenging. Although Hyperledger doesn't require gas fee structure, Ethereum gas fee leads to high transaction costs. Thus, the overall cost of the system can raise. The future research directions should focus on semantic interoperability of the EHRs. Further, natural language processing with deep learning models can be used to improve the accuracy and scalability of the method.

Ethics statements

Hepatitis dataset was used for this research. This dataset is freely available on https://archive.ics.uci.edu/dataset/46/hepatitis *. This dataset is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) license. This allows for the sharing and adaptation of the datasets for any purpose, provided that the appropriate credit is given. Dataset is cited at reference [36].*

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

CRediT authorship contribution statement

Rahul Ganpatrao Sonkamble: Methodology. **Anupkumar M. Bongale:** Methodology, Supervision. **Shraddha Phansalkar:** Methodology. **Deepak Sudhakar Dharrao:** Methodology, Supervision.

Acknowledgments

This research is supported by Symbiosis International (Deemed University).

References

[1] Z.H. Munim, O. Duru, E. Hirata, Rise, fall, and recovery of blockchains in the maritime technology space, J. Mar. Sci. Eng. 9 (3) (2021) 266.
[2] R. Belchior, A. Vasconcelos, S. Guerreiro, M. Correia, A survey on blockchain interoperability: past, present, and future trends, ACM Comput. Surv. (CSUR) 54 (8) (2021) 1–41.
[3] M. Madine, K. Salah, R. Jayaraman, Y. Al-Hammadi, J. Arshad, I. Yaqoob, Appxchain: application-level interoperability for blockchain networks, IEEE Access 9 (2021) 87777–87791.
[4] P.G. Lopez, A. Montresor, A. Datta, Please, do not decentralize the Internet with (permissionless) blockchains!, in: Proceedings of the 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS), IEEE, 2019, pp. 1901–1911.
[5] A. Lohachab, S. Garg, B. Kang, M.B. Amin, J. Lee, S. Chen, X. Xu, Towards interconnected blockchains: a comprehensive review of the role of interoperability among disparate blockchains, ACM Comput. Surv. (CSUR) 54 (7) (2021) 1–39.
[6] S.D. Kotey, E.T. Tchao, A.R. Ahmed, A.S. Agbemenu, H. Nunoo-Mensah, A. Sikora, E. Keelson, Blockchain interoperability: the state of heterogenous blockchain–to-blockchain communication, IET Commun. 17 (8) (2023) 891–914.
[7] Zarick, R., Pellegrino, B., & Banister, C. (2021). Layerzero: trustless omnichain interoperability protocol. arXiv preprint arXiv:2110.13871.
[8] L. Lys, A. Micoulet, M. Potop-Butucaru, R-SWAP: relay based atomic cross-chain swap protocol, in: Proceedings of the Algorithmic Aspects of Cloud Computing: 6th International Symposium, ALGOCLOUD, Lisbon, Portugal, September 6–7, 2021, Springer International Publishing, 2021, pp. 18–37. Revised Selected Papers 6.
[9] J. Zheng, D.K.C. Lee, D. Qian, An in-depth guide to cross-chain protocols under a multi-chain world, World Sci. Ann. Rev. Fintech 1 (2023) 2350003.
[10] Y. Pang, in: A New Consensus Protocol For Blockchain Interoperability Architecture, 8, IEEE Access, 2020, pp. 153719–153730.
[11] G. Wang, Q. Wang, S. Chen, Exploring blockchains interoperability: a systematic survey, ACM Comput. Surv. 55 (13s) (2023) 1–38.
[12] B. Pillai, K. Biswas, V. Muthukkumarasamy, Cross-chain interoperability among blockchain-based systems using transactions, Knowl. Eng. Rev. 35 (2020) e23.
[13] R. Tsepeleva, V. Korkhov, Building DeFi applications using cross-blockchain interaction on the wish swap platform, Computers 11 (6) (2022) 99.
[14] R.G. Sonkamble, S.P. Phansalkar, V.M. Potdar, A.M. Bongale, Survey of interoperability in electronic health records management and proposed blockchain based framework: myBlockEHR, IEEe Access 9 (2021) 158367–158401.
[15] M. Kaiser, From scalability to cross-chain DeFi, in: The Elgar Companion to Decentralized Finance, Digital Assets, and Blockchain Technologies, Edward Elgar Publishing, 2024, pp. 265–279.
[16] Augusto, A., Belchior, R., Correia, M., Vasconcelos, A., Zhang, L., & Hardjono, T. (2023). Sok: security and privacy of blockchain interoperability. Authorea Preprints.
[17] K. Zala, V. Modi, D. Giri, B. Acharya, S. Mallik, H. Qin, Unlocking Blockchain Interconnectivity: Smart Contract-Driven Cross-Chain Communication, IEEE Access, 2023.
[18] M. Nissl, E. Sallinger, S. Schulte, M. Borkowski, Towards cross-blockchain smart contracts, in: Proceedings of the 2021 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), IEEE, 2021, pp. 85–94.
[19] S. Velmurugan, M. Prakash, S. Neelakandan, E.O. Martinson, An efficient secure sharing of electronic health records using IoT-based Hyperledger blockchain, Int. J. Intell. Syst. (2024) 2024.
[20] W. Ou, S. Huang, J. Zheng, Q. Zhang, G. Zeng, W. Han, An overview on cross-chain: mechanism, platforms, challenges and advances, Comput. Netw. 218 (2022) 109378.

[21] S. Alzahrani, T. Daim, K.K.R. Choo, Assessment of the blockchain technology adoption for the management of the electronic health record systems, IEEe Trans. Eng. Manage 70 (8) (2022) 2846–2863.
[22] K.S. Alshudukhi, M.A. Khemakhem, F.E. Eassa, K.M. Jambi, An interoperable blockchain security frameworks based on microservices and smart contract in IoT environment, Electronics 12 (3) (2023) 776 (Basel).
[23] K.W. Prewett, G.L. Prescott, K. Phillips, Blockchain adoption is inevitable—Barriers and risks remain, J. Corp. Account. Finance 31 (2) (2020) 21–28.
[24] R.G. Sonkamble, A.M. Bongale, S. Phansalkar, A. Sharma, S. Rajput, Secure data transmission of electronic health records using blockchain technology, Electronics 12 (4) (2023) 1015 (Basel).
[25] R. Cerchione, P. Centobelli, E. Riccio, S. Abbate, E. Oropallo, Blockchain's coming to hospital to digitalize healthcare services: designing a distributed electronic health record ecosystem, Technovation 120 (2023) 102480.
[26] O.R. Akinyemi, M.N. Sibiya, O. Oladimeji, Communication model enhancement using electronic health record standard for tertiary hospital, S. Afr. J. Inf. Manage 24 (1) (2022) 1472.
[27] P. Zhang, D.C. Schmidt, J. White, G. Lenz, Blockchain technology use cases in healthcare, in: Advances in Computers, 111, Elsevier, 2018, pp. 1–41.
[28] J. Ducrée, M. Etzrodt, S. Bartling, R. Walshe, T. Harrington, N. Wittek, J. Lawton, Unchaining collective intelligence for science, research, and technology development by blockchain-boosted community participation, Front. Blockchain 4 (2021) 631648.
[29] P.P. Ray, Web3: a comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions, Internet Things Cyber-Phys. Syst. 3 (2023) 213–248.
[30] F.A. Reegu, M.O. Al-Khateeb, W.A. Zogaan, M.R. Al-Mousa, S. Alam, I Al-Shourbaji, Blockchain-based framework for interoperable electronic health record, Ann. Rom Soc. Cell Biol. (2021) 6486–6495.
[31] D. Horgan, J. Hackett, C.B. Westphalen, D. Kalra, E. Richer, M. Romao, A. Montserrat, Digitalisation and COVID-19: the perfect storm, Biomed. Hub. 5 (3) (2020) 1–23.
[32] I. Yaqoob, K. Salah, R. Jayaraman, Y Al-Hammadi, Blockchain for healthcare data management: opportunities, challenges, and future recommendations, Neural Comput. Appl. (2022) 1–16.
[33] M. Abdalla, Password-based authenticated key exchange: an overview, in: Proceedings of the Provable Security: 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10, 2014, Springer International Publishing, 2014, pp. 1–9.
[34] K. Shuaib, J. Abdella, F. Sallabi, M.A. Serhani, Secure decentralized electronic health records sharing system based on blockchains, J. King Saud Univ. Comput. Inf. Sci. 34 (8) (2022) 5045–5058.
[35] A. Haddad, M.H. Habaebi, F.E.M. Suliman, E.A. Elsheikh, M.R. Islam, S.A. Zabidi, Generic patient-centered blockchain-based EHR management system, Appl. Sci. 13 (3) (2023) 1761.
[36] J. Jayabalan, N. Jeyanthi, Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy, J. Parallel. Distrib. Comput. 164 (2022) 152–167.
[37] K. Miyachi, T.K. Mackey, hOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design, Inf. Process. Manage 58 (3) (2021) 102535.
[38] IPFS, Accessed on: February 2024, [Online]. Available https://ipfs.tech/.
[39] Ethereum, Accessed on: February 2024, [Online]. Available https://ethereum.org/en/.
[40] Hyperledger Foundation, Accessed on: March 2024, [Online]. Available https://www.hyperledger.org/projects/fabric.
[41] F. Hashim, K. Shuaib, E. Baraka, F. Sallabi, Enhancing EHR sharing through interconnected blockchains via global smart contracts, Int. J. Comput. Digit. Syst. 15 (1) (2024) 1–13.
[42] Javan, R., Mohammadi, M., Beheshti-Atashgah, M., & Aref, M.R. (2024). A scalable multi-layered blockchain architecture for enhanced EHR sharing and drug supply chain management. arXiv preprint arXiv:2402.17342.
[43] [Hepatitis, (1988), UCI Machine Learning Repository, Accessed on: March 2024, [Online]. Available https://archive.ics.uci.edu/ml/datasets/hepatitis.
[44] Getting started with MetaMask, Accessed on: February 2024, [Online]. Available https://support.metamask.io/hc/en-us/articles/360015489531-Getting-started-with-MetaMask.
[45] Networks, Accessed on: February 2024, [Online]. Available https://ethereum.org/en/developers/docs/networks/#testnets.
[46] Ultimate Guide to Truffle: the Gateway to Full Stack Blockchain Development., Accessed on: April 2024, [Online]. Available https://trufflesuite.com/guides/ultimate-guide-to-truffle-the-gateway-to-full-stack-blockchain-development/.