

# Decentralized Electronic Health Records (DEHR): A Privacy-preserving Consortium Blockchain Model for Managing Electronic Health Records

Mahdi Ghadamyari<sup>a</sup> and Saeed Samet

*Department of Computer Science, University of Windsor, Windsor, Canada*

**Keywords:** Blockchain, Healthcare, Smart Contract, Hyperledger Fabric, Electronic Health Records.

**Abstract:** Blockchain applications have proven the potential of this disruptive technology to achieve a disintermediated model for improving efficiency and reducing the additional costs. The de facto healthcare applications suffer from lack of interoperability, which is a result of using traditional centralized platforms that create private data silos with poor interoperability and a high maintenance cost. In this paper, we introduce a blockchain-based Decentralized Electronic Health Records (DEHR) model that enables healthcare providers to control their electronic health records and share them among other organizations involved in the system in a secure and consortium manner.

## 1 INTRODUCTION

Lack of interoperability in healthcare systems not only costs patients and health providers millions but also costs lives. A survey by Deloitte in 2018 ("Stephanie Newkirchen, 2018) from 624 US primary care and specialty physicians shows that interoperability has remained the top demand from physicians as 62 percent of physicians say that interoperability needs improvement just as they said before in a 2016 survey. Another survey by Deloitte in 2018 (sur, 2018), reported that 74 percent of the more than 1,000 executives worldwide believe that their organizations see a "compelling business case" for the use of blockchain. These surveys demonstrate how blockchain is changing the industry and the importance of having a compatible and interoperable health care platform. However, healthcare is far behind from modern technologies, especially when it comes to leveraging new technologies such as blockchain.

Blockchain technology can be used to connect health providers and facilitate data sharing within organizations. It adds transparency and immutability to the data and enables the peer-to-peer transfer of digital assets such as Electronic Health Records (EHRs). In this work, we introduce a model for managing EHRs based on a consortium blockchain network. In our model, organizations such as health providers can register their staff and patients in the system and con-


trol access to the health records. Professionals can request for limited or unlimited access to a patient's data. Also, other organizations can transfer a patient to their organization and take control of the patient's health records. To make our model in compliance with privacy acts, we utilize access control lists (ACLs) and define policies to manage access to the resources. We implemented and evaluated this model, using several performance testing measures.

The rest of the paper is organized as follows: I) An overview of similar works, II) Definitions, III) structure of our model, IV) Implementation and experimental results V) Discussions VI) Conclusions.

## 2 RELATED WORK

Following, we briefly review some of the research works related to blockchain adoption in health record management systems.

The authors in (Azaria et al., 2016) proposed a blockchain-based and decentralized health records management system called MedRec. They used a public blockchain that incentives researchers to mine new blocks in exchange for getting access to anonymized medical data. The authors claimed that their proposed system increases the transparency of medical records, the stability of the network, and the confidentiality of data. The mining process is necessary for having a secure network in public blockchains; however, it is a time-consuming pro-

<sup>a</sup>  <https://orcid.org/0000-0003-2105-9901>

cess and requires a high computation power. Besides, transaction processing time mainly depends on the number of available miners willing to mine the pending transactions, which currently can take up to 5 minutes.

The MedRec (Azaria et al., 2016) work was later continued by the authors in (Nchinda et al., 2019). The authors replaced miners with a network of trusted providers that participate in a proof of authority consensus mechanism. They used blockchain to store permission contracts. In their work, providers can join the network and grant patients, and other entities access to their databases using their credentials.

The authors in (Mikula and Jacobsen, 2018) used a federated and private blockchain to explore an auditable identity and access management framework for EHR systems. Evaluation of their system showed a size of 3.8 MB for the initialization of the blockchain with 2-3 seconds of mining time for new transactions.

The authors in (Chen et al., 2019) presented an integration of a cloud and blockchain storage scheme to manage PHR data. They used off-chain cloud storage for storing a large amount of medical data and the blockchain for indexing and securing them. In their work, patients are in control of their data. However, the interoperability of their system is not examined.

In (Abouzahra, 2019), the authors proposed an interactive model for a blockchain-based PHR system. In the proposed system, smart contracts are utilized to collect patients' health records, and blockchain technology is used to make transactions immutable and traceable. The authors claimed that their approach encourages physicians to have more engagement with their patients outside clinics resulting in better care delivery.

### 3 DEFINITIONS

There are two types of blockchains: permissionless (public) and permissioned (private/consortium) (Alhadhrami et al., 2017). Depending on the need, each blockchain type has its advantages and disadvantages.

In public blockchains, anyone can join the network, invoke transactions, write new blocks, and contribute to the maintenance of the network. On the one hand, this feature adds transparency to the data and makes the data extremely secure and immutable. On the other hand, redundancy in the network makes the network slower and increases the maintenance cost, significantly. Public blockchains are most suitable for public digital assets such as cryptocurrencies, where everyone needs access to read the ledger. However,

this level of transparency might endanger the privacy of users. Bitcoin (Nakamoto et al., 2008) and Ethereum (Wood et al., 2014) are two well-known examples of public blockchains.

On the contrary, permissioned blockchains only allow the pre-authorized participants to maintain the ledgers and give access or add users to the network. Permissioned blockchains can easily scale and have significantly faster transaction processing time in exchange for the anonymity of the users. Further, since the ledger is not open to the public, users in the network have a higher level of privacy. Permissioned blockchains can be categorized into two types: private and consortium. In private blockchains, only one participant has the right to add blocks to the chain or allow others to read the transactions. In consortium blockchains, a set of organizations control the consensus process. Also, blocks can be added to the chain only if the predefined nodes reach a consensus. For an EHR system, a consortium blockchain is more appealing mainly because of the faster transaction processing time and the higher level of privacy that it offers to the participants in the system.

There are two major frameworks for deploying a consortium blockchain network: 1) Quorum (Quorum, 2019), which is an enterprise-focused version of Ethereum, and 2) Hyperledger Fabric (Androulaki et al., 2018), a product by Linux Foundation which is supported by enterprise companies like IBM, Intel, and SAP. In our work, we use Hyperledger Fabric for model implementation because of its bigger community of developers, support from large enterprise companies, and a wide variety of APIs.

There are five main concepts in a Hyperledger Fabric model: assets, participants, transactions, chaincodes, and access control lists (ACLs). Participants are the users involved in the model, such as patients and practitioners. Assets are tangible or intangible properties that participants can own, such as health records.

Transactions are abstract actions and trigger a chaincode to modify the ledger. Chaincodes (or smart contracts) are a set of procedures defined by the blockchain network designer to process inputs and alter the resources. Examples of transactions are transferring a patient to another organization or granting permissions. Access control lists are a set of rules that can be defined to control access to different operations on resources.

All permission managements are handled through chaincodes and access control lists and are enforced by all participating nodes in the network.

## 4 SYSTEM DESIGN

Our model consists of three participant types, two asset types, and three transactions. The three types of participants are organizations, professionals, and patients. The two types of assets are health records and permission requests. The three transactions are 1) Patient transfer transaction: for transferring a patient to another organization, 2) Permission request transaction: for requesting access to health records, and 3) Change permission request status transaction: To grant or deny a permission request.

Organizations can create records for their patients or transfer an already existing patient in the system by sending a transfer transaction. In the following sections, we will describe each part in detail.

### 4.1 Health Record Asset

Health records are consisting of five parameters: health record ID, record type, details, and links to the patient and the organization.

Health record ID is the default identifier of the record. Record type determines the type of the record and is naturally an enumerated type. Examples of record types are identity, prescriptions, lab results, vaccines, etc. Detailed information related to the record, such as medicine and dosage, will be stored in the "Details" parameter. Listing 1 shows a sample health record.

Listing 1: A Sample Health Record.

```
{
  "$class": "org.DEHR.HealthRecord",
  "healthRecordId": "577",
  "recordType": "IDENTITY",
  "details": "{SIN:111111111, Father: 'Bob'}",
  "patient": "resource:org.DEHR.Patient#1",
  "organization": "resource:org.DEHR.Organization#2"
}
```

Permissions for CRUD (Create, Read, Update, Delete) operations on health records will be controlled by Hyperledger Access Control Lists (ACLs). Upon submitting an operation, an ACL script will be executed to verify that the participant has the permission to run that operation. Figure 1 shows the flow for CRUD operations on health records.

### 4.2 Permission Request Transaction

To access health records, professionals must have required permissions. Permissions can be granted by

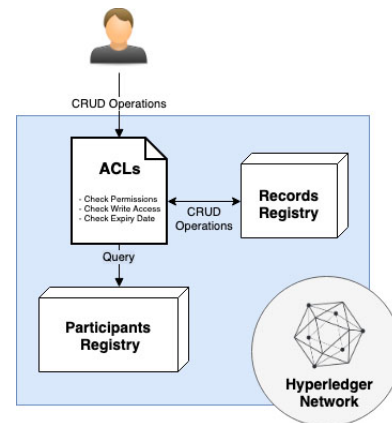


Figure 1: CRUD Operation Flow for a Health Record.

the organization that the patient is associated with. There are five parameters that need to be determined prior to send a permission request:

1. Record Types: Various types of health records can be created for a patient. It is essential to grant permissions based on their types to preserve privacy. As part of a permission request, professionals may determine what record types they need to have access to using this parameter. A null value for this parameter grants the professional access to all types of records belong to that patient.
2. Write Access: This parameter determines whether the professional should have access to add a new record or modify an already existing record for the patient in question. This parameter, along with the record types parameter, will be used by the access control rules to determine the write access for a professional.
3. Status: Permissions can be denied, granted, or revoked. This parameter determines the current state of permission, which by default is set to "Pending".
4. Expiry Date: A permanent access to a health record might not always be desired. This parameter can be defined to determine an expiry date for the associated permission. Expirations will be enforced by access control rules embedded in the blockchain, automatically.
5. Patient: The patient that owns the health record will be linked in this parameter. Chaincodes and access control rules use this parameter to access the patient.

By calling the "RequestPermission" transaction with the above parameters, a new "Permission Request" asset will be instantiated and assigned to the professional participant (Listing 2). By using the Hyperledger events feature, organizations and patients

can be automatically notified about the new permission request.

Listing 2: A sample permission request transaction.

```
{
  "$class": "org.dehr.RequestPermission",
  "permission": {
    "$class": "org.dehr.Permission",
    "recordType": ["MEDICATION"],
    "writeAccess": true,
    "patient": "resource:org.dehr.Patient#10"
  },
  "professional": "resource:org.dehr.Professional#1"
}
```

After submitting a permission request, the organization that controls the health record(s) can either accept or deny the request by calling the "ChangePermissionStatus" transaction. (Listing 3).

Listing 3: A sample respond to a permission request.

```
{
  "$class": "org.dehr.ChangePermissionStatus",
  "permissionRequest": "resource:org.dehr.PermissionRequest#1",
  "status": "GRANTED"
}
```

This transaction triggers a set of chaincodes to update the status of the related permission request asset and also add or remove the permission from the professional participant's record.

### 4.3 Transfer Patient Transaction

To transfer a patient, organizations can invoke the "TransferPatient" transaction. Listing 4 shows a sample "TransferPatient" transaction that transfers the patient to another organization.

Listing 4: A sample transfer request transaction.

```
{
  "$class": "org.dehr.TransferPatient",
  "patient": "resource:org.dehr.Patient#2",
  "organization": "resource:org.dehr.Organization#4"
}
```

### 4.4 Access Control Lists

Access Control Lists (ACLs) can be used to manage access to different operations (Read, Write, Update, and Delete) on resources. We use ACLs to enforce

permissions declared by chaincodes and stored in participants and assets records. Listing 5 shows a sample ACL function that permits authorized professionals reading access to health records. The function validates the record type, patient, and expiry date of the permission and returns a boolean, which determines the final decision.

Listing 5: ACL for granting authorized professionals read access to health records.

```
function healthRecordsACL(
  professional, record) {
  return professional.
    grantedPermissions.some(
      function(grantedPermission) {
        const permission =
          grantedPermission.permission;
        return (
          permission.recordType.indexOf(
            record.recordType) >= 0 &&
          permission.patient.
            getIdentifier() === record.
            patient.getIdentifier() &&
          (!permission.expiryDate ||
            new Date() < new Date(
              permission.expiryDate.
                getTime()))
        );
      });
}
```

## 5 EXPERIMENTAL RESULTS

We implemented the model using Hyperledger Composer and Hyperledger Fabric framework. The model includes chaincodes for the three transactions that were discussed in the previous section, access rules, and the business model. We performed several performance testings to evaluate the scalability and response time of different features of our platform. We used an OS X machine with a 3.5 GHz Intel Core i7 CPU and 16 GB 2133 MHz LPDDR3 memory during our experiments.

We created a blockchain database with an entry of 10,000 patients. In this database, a single query from the patients' registry took 252 ms, and calling the patient transfer transaction took 2399ms to process. We extended the experiment and simulated up to 100 concurrent users and computed the median response times of the network [Figure 2]. The experiment shows a faster growth in transaction processing time with an increase in the number of active users. This behavior shows that the mining process takes more time with an increase in the number of pending transactions.

Table 1: Performance Results Based on the Number of Entries ( $N$ ).

| Action             | Mean $\pm$ Standard Deviation (s) |                    |                    |
|--------------------|-----------------------------------|--------------------|--------------------|
|                    | $N < 6k$                          | $N \in [6k, 10k]$  | $N \in [10k, 14k]$ |
| Add patient        | $2.512 \pm 0.072$                 | $2.521 \pm 0.041$  | $2.523 \pm 0.038$  |
| Delete patient     | $2.508 \pm 0.054$                 | $2.522 \pm 0.053$  | $2.508 \pm 0.051$  |
| Transfer patient   | $2.380 \pm 0.037$                 | $2.381 \pm 0.039$  | $2.379 \pm 0.035$  |
| Request permission | $2.477 \pm 0.074$                 | $2.435 \pm 0.0435$ | $2.426 \pm 0.047$  |
| Grant permission   | $2.470 \pm 0.924$                 | $2.455 \pm 0.126$  | $2.373 \pm 0.353$  |
| Query patient      | $0.154 \pm 0.021$                 | $0.156 \pm 0.018$  | $0.157 \pm 0.019$  |

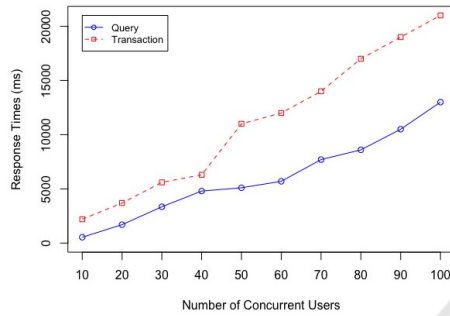


Figure 2: Query and Transaction Processing Time per Active User for the Proposed EHR Model.

In the next experiment, we gradually added 14,000 of various resources in the network and computed the average response time of sending queries and invoking transactions.

The result [Table 1] shows a relatively consistent response time, which indicates that the number of stored records does not remarkably affect the processing time of mining a new block.

## 6 DISCUSSION

The immutability of data can be considered as one of the most important features of blockchains. Blocks are chained and secured with hashes to immune the ledger against any manipulations. However, this may not always be an acceptable feature. Many privacy acts grant patients the right to correct their data or to instruct health information custodians not to share their personal health information with others. In public blockchains that ledgers are shared and open to the public, one approach to comply with privacy acts is to store identifiable data in a separate secure database and only store anonymized data in blockchains and linking them using a unique identifier. This approach is used in MedRec (Azaria et al., 2016). In private blockchains, access to health records can be precisely controlled and granted only with the consent of patients. Besides, while the history of a ledger cannot be

modified, access to the history of changes can be managed and restricted to the patient. Another approach is to use the private data feature offered in the Hyperledger Fabric platform. Hyperledger fabric stores a hash of the private data on the public ledger as a shred of evidence for the existence of the data. Later, private data can be destroyed by the authorized authorities and become inaccessible permanently from the blockchain.

## 7 CONCLUSIONS

In this work, we proposed a Privacy-Preserving Decentralized EHR platform based on a permissioned blockchain framework. In our model, different organizations involved in the health care industry can join the network; they can add their staff and patients in the network and manage the electronic health records. We have introduced chaincodes for transferring a patient, controlling access to health records based on record types, and access controls for automatically revoking permissions after their expiry date. In future works, we will further examine the scalability of our model, try to improve the efficiency and investigate solutions for integration of legacy systems with the proposed model.

## REFERENCES

- (2018). Deloitte survey: For blockchain-savvy executives, movement expected over next year and 'pragmatism' the new mindset. <https://www.prnewswire.com/news-releases/deloitte-survey-for-blockchain-savvy-executives-movement-expected-over-next-year-and-pragmatism-the-new-mindset-300648480.html>.
- (2019). Quorum. [www.jpmorgan.com/global/Quorum](http://www.jpmorgan.com/global/Quorum).
- Abouzahra, M. (2019). Using blockchain technology to enhance the use of personal health records.
- Alhadhrami, Z., Alghfeli, S., Alghfeli, M., Abedlla, J. A., and Shuaib, K. (2017). Introducing blockchains for

- healthcare. In *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)*, pages 1–4. IEEE.
- Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the Thirteenth EuroSys Conference*, page 30. ACM.
- Azaria, A., Ekblaw, A., Vieira, T., and Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*, pages 25–30. IEEE.
- Chen, Y., Ding, S., Xu, Z., Zheng, H., and Yang, S. (2019). Blockchain-based medical records secure storage and medical service framework. *Journal of medical systems*, 43(1):5.
- Mikula, T. and Jacobsen, R. H. (2018). Identity and access management with blockchain in electronic healthcare records. In *2018 21st Euromicro Conference on Digital System Design (DSD)*, pages 699–706. IEEE.
- Nakamoto, S. et al. (2008). Bitcoin: A peer-to-peer electronic cash system.
- Nchinda, N., Cameron, A., Retzepi, K., and Lippman, A. (2019). Medrec: A network for personal information distribution. In *2019 International Conference on Computing, Networking and Communications (ICNC)*, pages 637–641. IEEE.
- ”Stephanie Newkirchen, N. E. (2018). Electronic health records: Can the pain shift to value for physicians? <https://www2.deloitte.com/us/en/insights/industry/health-care/ehr-physicians-and-electronic-health-records-survey.html>.
- Wood, G. et al. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32.