HIGH SCHOOL EDITION
Journal of Student Research
Volume 12 Issue 3 (2023)

Blockchain Based Decentralized Healthcare Network to Share Electronic Medical Records

Anoushka Iyer

Irvington High School

ABSTRACT

Over 172 ransomware attacks on US healthcare organizations since 2016 have cost over $157 million total and disrupted care for over 70% of patients impacted, prompting healthcare CIOs to declare cyberattacks as one of the most devastating healthcare issues today. Furthermore, lack of interoperability of patient data between healthcare providers prevents patients from exploring care outside their provider's network. Though hospitals utilize electronic health records (EHR), data formats remain fragmented and non-interoperable, leaving patients to be responsible for transporting their own data between providers or insurance plans. Permissioned blockchain technology can solve both these issues due to its inherent transparency, immutability and data sharing capabilities. Therefore, I developed a decentralized application called HyperEHRbase that would allow patients to control their own health records and share them with different healthcare providers. My application extends an open-source OpenEHR implementation called ehrbase. Unlike ehrbase, my application writes health records into a Hyperledger blockchain, not a centralized database. The blockchain network is designed to work as a decentralized healthcare network, allowing patients and healthcare providers to mutually exchange data. Patients can register to the healthcare network using their personal devices and voluntarily grant multiple healthcare providers access to their medical records. Doctors and other care providers can also register to the network and access information shared by patients. This system secures electronic healthcare records in an immutable blockchain and makes them interoperable using the OpenEHR standard. Patients will also have control over their data, which is a significant improvement over the current healthcare system.

Research Question

The main research question is to evaluate whether blockchain technology is suitable to store patient healthcare records rather than the traditional method of a database. My aim is to create a blockchain-based hospital information system. Secondly, I want to explore if blockchain technology will make such a healthcare system secure from cyber attacks. Finally, I would like to design my system so that patients can share their data across organizations.
By addressing these questions, my research builds a design for a decentralized healthcare system that stores patient records into a blockchain network but maintains security and privacy between patients and healthcare providers to securely access this data. Today, healthcare systems are implemented as centralized systems with data stored in databases. Electronic healthcare records such as patient blood tests and MRI scans are stored in databases at each healthcare provider, and are not interoperable between providers.

Prior Research in this Area

Blockchain technology has been used successfully to implement digital citizen identities in the UK. It has also been used to build a digital healthcare system in Estonia.

In a 2019 study, the authors propose a blockchain-based platform to share electronic medical records (EMR), but the scope of their project is across different departments of a single hospital, called a "smart hospital" (Jamil et al. 2019). In another study, the authors propose a similar platform for patients to share their electronic records with doctors from different networks, but their project proposes a public blockchain, as opposed to a private, permissioned blockchain (Celesti et al. 2020). The former has distinct disadvantages compared to the latter in terms of performance and security.

In this study, the authors also propose an inter-hospital EMR sharing proposal via blockchain, but the emphasis of their project is on smart contracts between the hospitals (Celesti et al. 2020). They make no mention of the format of the electronic records, which is vital for widespread interoperability across providers.
Some nascent commercial implementations also exist that propose similar sharing of patient records via blockchain, but they create more "walled gardens" of commercial blockchain networks.

Conceptions and Notation

Interoperability of Healthcare Records

- Electronic Healthcare Records (EHR) are not interoperable between healthcare providers because each provider uses a centralized healthcare information system.
- Centralized EHR systems are sold by commercial vendors as "walled gardens".
- The lack of government norms or regulations leaves providers with no incentives to make data interoperable, causing patients to suffer.

Blockchain in Healthcare

- California's Blockchain Working Group published a report in October 2020 suggesting digital healthcare as an area where blockchain technology would be useful (Crittenden).
- Early usage of blockchain in healthcare includes MediLedger in the US, Digital Healthcare in Estonia, and MedicalChain in the UK ("UK Digital Identity and Attributes Trust Framework - Beta Version").

Notation

Blockchain is a distributed ledger system. Copies of the ledger are stored in separate computers that share and synchronize transactions. Thus, data storage is decentralized.

Permissioned vs Public blockchain: Public blockchains are open to anyone to access them whereas permissioned blockchains are only accessible to those who have been invited to participate by the administrators of those networks.

Smart contract: The code that contains the logic for executing the agreement of data sharing between nodes in a blockchain network.

Chaincode: the deployable smart contract package that is installed on the peer nodes and deployed onto the channel.

Ordering Service: Ordering nodes together arrive at a consensus on the order in which transactions should be added to the ledger. Ordering is important because peers may be running far away from each other and not have the same view of when a transaction occurred. Ordering is what differentiates a permissioned blockchain from a public one like Ethereum.
Peer nodes: Peer nodes are vital to Hyperledger fabric systems. They have the following responsibilities:

1. Store blockchain ledger
2. Validate transactions before they are committed to the ledger
3. Run smart contracts

Channel: A layer of private communication between certain nodes in a blockchain. For instance, a channel for healthcare providers and patients only, a channel for healthcare providers and insurance companies.

Electronic Health Records: Electronic health records (EHR) are digital versions of a patient's health history, including diagnoses, medications, treatment plans, immunization history, vaccination history, allergies, and lab test results.
OpenEHR: OpenEHR is the name of a technology consisting of open specifications for patient health information that can be exchanged between independent entities in a technology-neutral and vendor-neutral fashion.

How Blockchain Works

As each transaction occurs, it is recorded by a peer node as a "block" of data.

- Those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual).
- The data format is customizable to store the information of choice: who, what, when, where, how much and even conditions— such as blood test results.

Each block is connected to the ones before and after it.

- These blocks form a chain of data as an asset moves from place to place or ownership changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks link securely together making them immutable and preventing a block from being inserted between two existing blocks.

Transactions are blocked together in an irreversible chain.

- Each additional block strengthens the verification of the previous block and hence the entire blockchain. This renders the blockchain tamper-evident, delivering the key strength of immutability.
- This removes the possibility of tampering by a malicious party and builds a ledger of transactions with integrity.

Project Design

The components of this system are described below.

Blockchain Network

The blockchain network is designed to be run by a reputed authority, like the State of California. This could be marketed by the government authority as the healthcare system for all resident patients and doctors in the state. The advantages of the network to patients include the control over their healthcare data and ability to share information between various healthcare providers, thereby getting a level of care that exceeds what is feasible today.

I explored three choices for the blockchain platform - Ethereum, Hyperledger Fabric, and Corda (Abrol). Of the three, I selected Hyperledger Fabric as the underlying implementation due to published research stating its strong access control mechanisms, higher performance, and broad applications to multiple industries.

- Step A1: Hyperledger 2.2 was downloaded and installed from the Hyperledger Fabric website. Prerequisites like Java, Golang, Git, curl and Docker were installed on my laptop per instructions on the website.
- Step A2: A 3 node network was brought up communicating over the Hyperledger blockchain. The three nodes include an ordering node and two peer nodes exchanging information over the network (role-playing two providers sharing data).

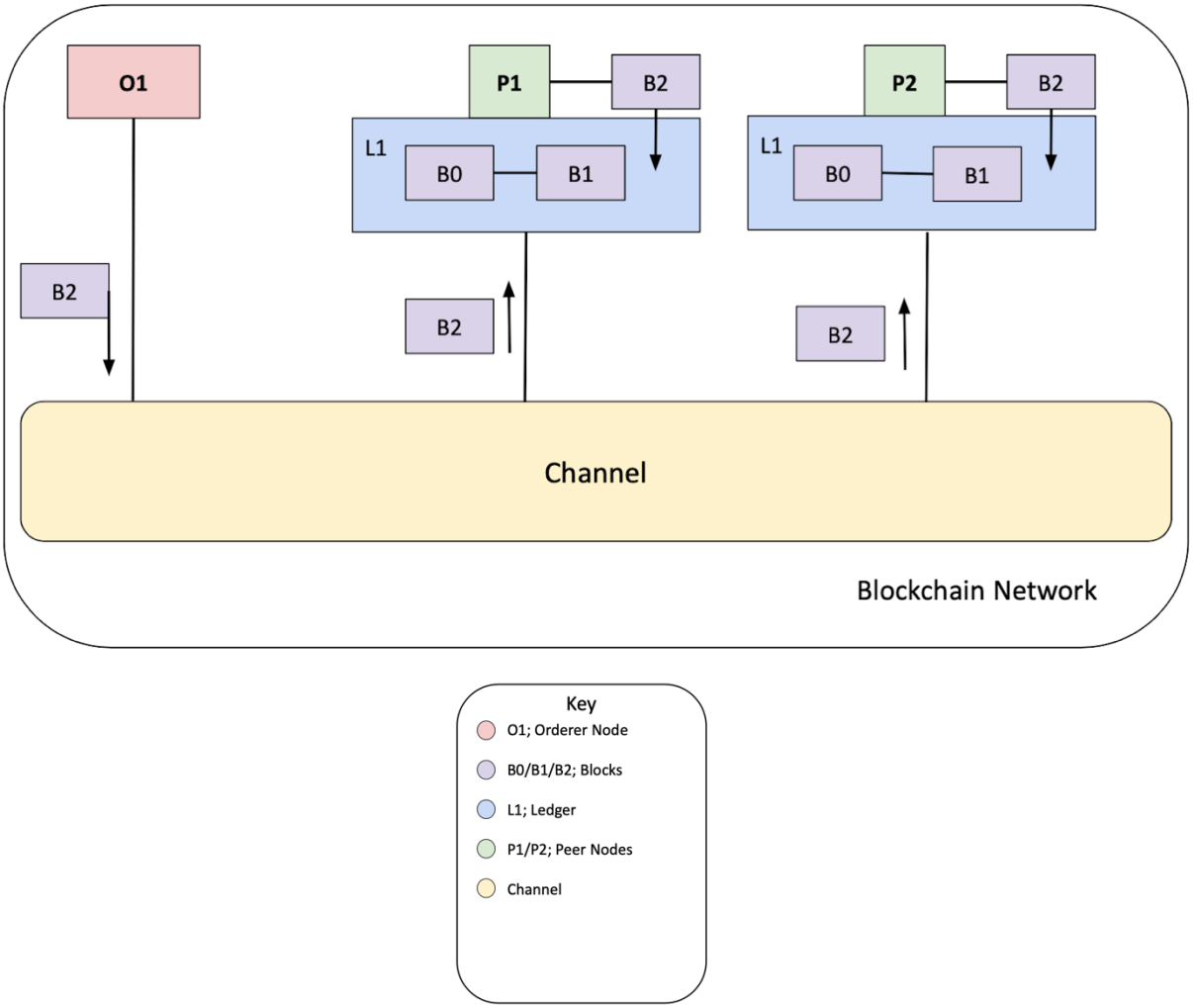

Figure 1: Project Design

Electronic Healthcare Records

- Step B1: Open standard OpenEHR was researched to explore its data specifications for storing patient records. Several specifications were noted for storing various types of medical information. I selected the specification for blood pressure to be implemented and stored in our blockchain network.

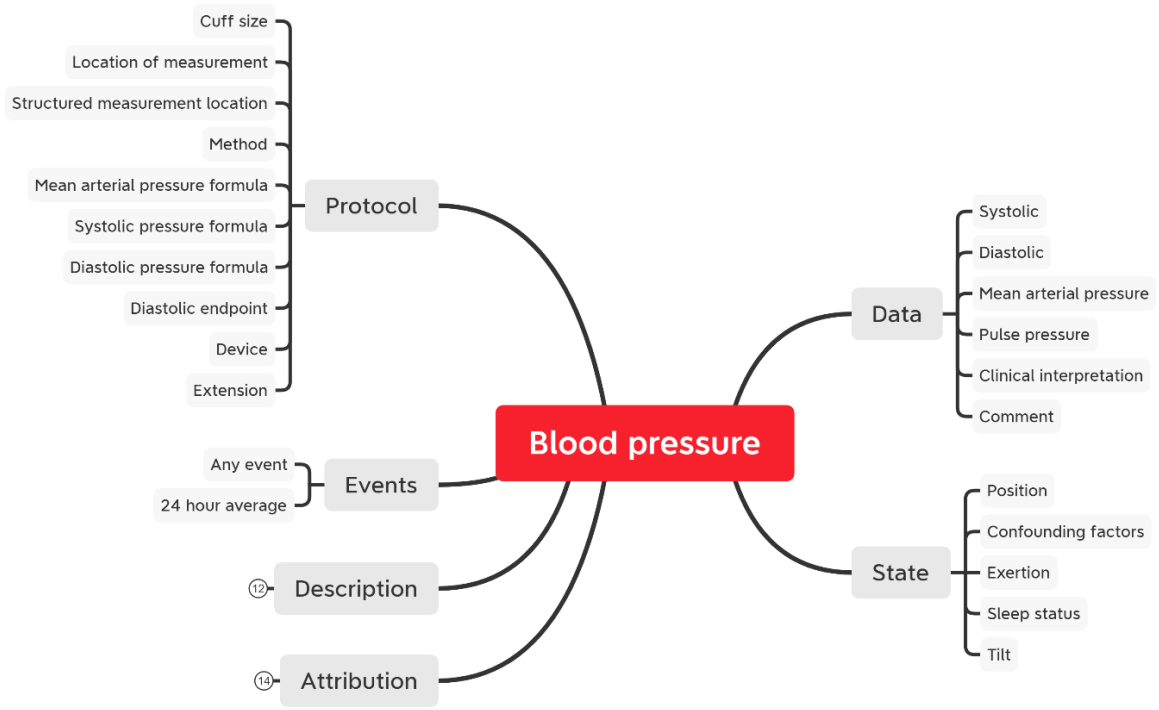

Figure 2: Blood Pressure open specification: courtesy OpenEHR specifications

- Step B2: A smart contract was developed to implement this blood pressure specification in our blockchain. Code was written in golang to implement this. The smart contract included functions to create blood pressure EHR records, update EHR records, delete records and clone records.
- Step B3: Sample data was generated to be stored in the blockchain network. I used the blood pressure test data standard from OpenEHR to generate sample data.
- Step B4: Smart contract and test data were compiled and converted into a deployable package to be pushed to the blockchain network.
- Step B5: The smart contract chaincode package was deployed to the 3-node network for communication between the peer nodes using a channel called “mychannel”.

Storing and accessing electronic healthcare records

- Step C1: Once the smart contract chaincode package was deployed to the 3-node network, test data was loaded to the network. This included 8 patient records with blood pressure test results.
- Step C2: Peer node org1 was able to access the test data loaded to the network.
- Step C3: Peer node org1 enabled data access to peer node org2.
- Step C4: Peer node org2 was verified to be able to access data shared by org1.

Transaction Flow Chart

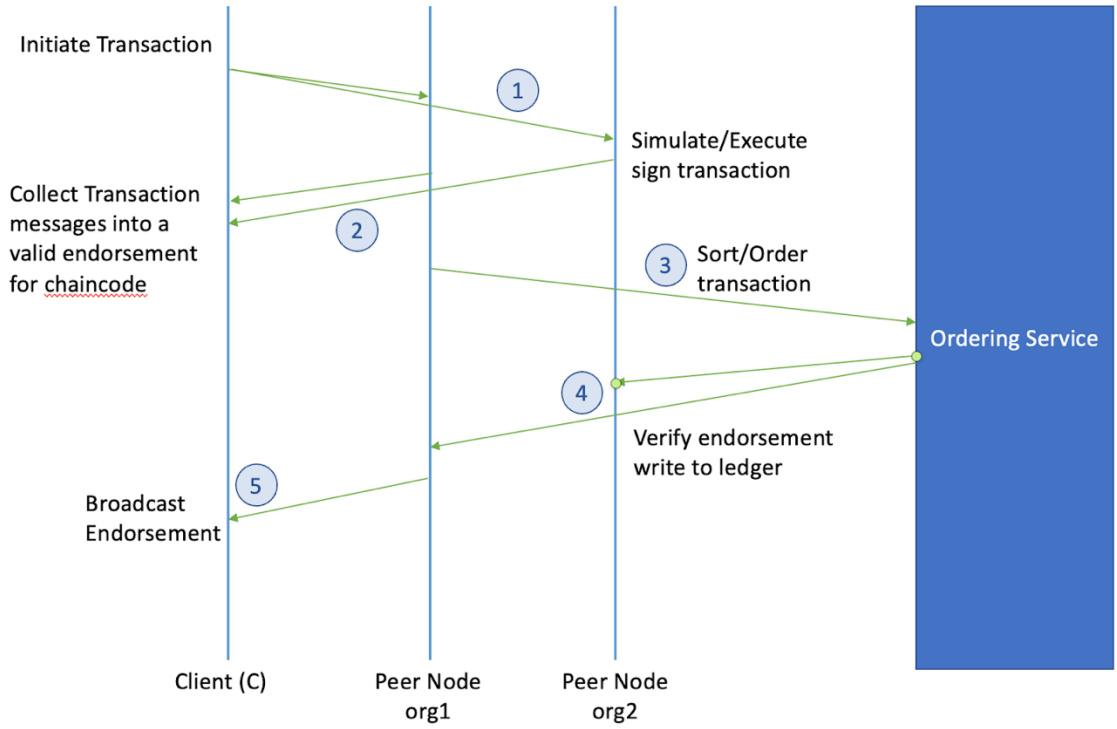

Figure 3: Transaction Flow Chart between participants of the blockchain network

Results

- I developed a decentralized healthcare application using an open standard (OpenEHR) that any healthcare provider can easily adopt and implement. OpenEHR is a well-published standard backed by several technology leaders (e.g. Microsoft, Ernst & Young) as well as healthcare networks in the US and Europe.
- The data will be stored on an immutable ledger that only authorized nodes (healthcare providers) can access and update.
- The application enables transportability of patient medical records between providers by giving patients full control over their data.

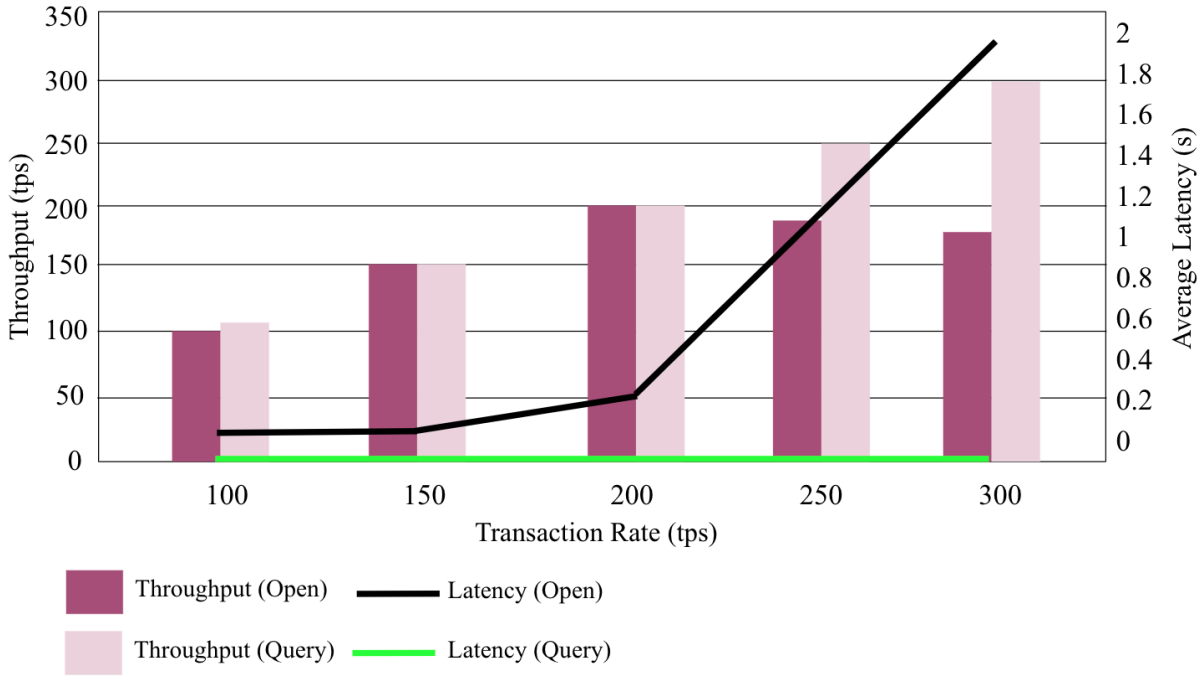

Figure 4: Performance Testing

The graph above depicts the throughput and latency, which are performance metrics for the system. The comparison shown is between my OpenEHR system and the traditional database query. Throughput is the number of transactions per second and latency is the time in seconds required for the transactions to occur.

The dark pink bars for the open system show a much lower latency, particularly at higher transaction rates. As the transaction rate increases, the latency for the query system is much higher than the latency of the open system. The black line plot of the open system has a much steeper slope for higher transaction rates, while the green line plot of the query based system stays flat for higher transaction rates. Therefore, it is conclusive that the OpenEHR system has a much better performance than the traditional query based system.

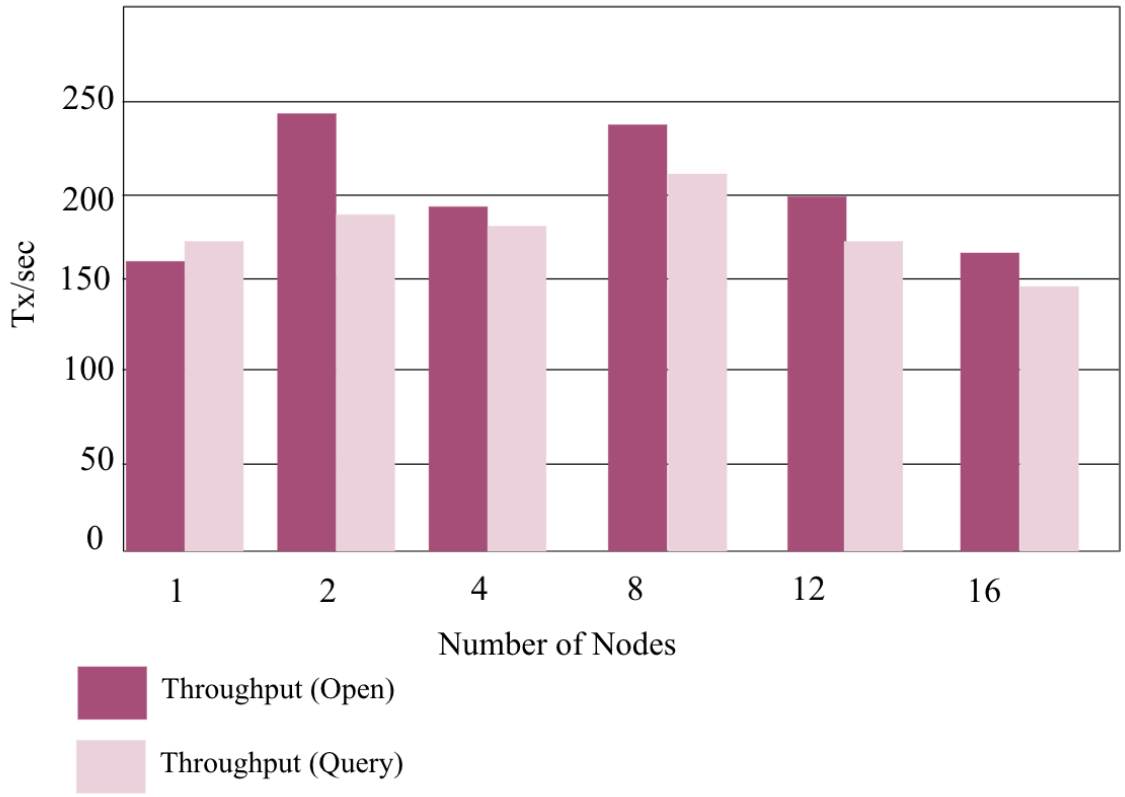

Figure 5: Throughput v. Nodes

The graph above depicts the comparison of the throughput (Tx/s) versus the number of nodes for my OpenEHR system and the traditional query based system. As the number of nodes increases, the throughput for the OpenEHR system is considerably greater than that of the traditional query-based system. This indicates once more that the OpenEHR system has an improved performance even with more nodes participating in the system.

Conclusion

- Patient Ownership: Patients are in control of their healthcare data and can access their data whenever they want, and share it with whoever they choose to.
- Open Standard: Healthcare data stored in the blockchain is based on an open standard (OpenEHR), allowing any healthcare provider to consume or publish records.
- Tamper Protection: Healthcare records are stored in the blockchain, making them immutable and resistant to tampering.

Limitations

- I had to run performance tests on the model with small samples of patient data that were likely unrealistic representations of real-world patient data at high volume.

- I only implemented the blood pressure test data standard from OpenEHR. This represented a reasonably complex form of patient data containing several parameters. There are numerous other patient healthcare data types that must be implemented similarly for a real-world implementation.

Future Research

- Use web or mobile apps (iOS or Android) to show patients being able to access and control healthcare data from personal apps.
- Healthcare regulation needed to nudge/push providers to adopt an open standard to share records with each other.
- Security and privacy might be raised as concerns by providers or consumer privacy groups. Appropriate education content might need to be put together to address concerns. Additional security or privacy steps to store data can also be taken.

Final Remarks

- My application is an asset to the healthcare industry due to its drastic improvement on current methods of medical record storage.
- This implementation will reduce the risk of cyberattacks on hospital systems by making patient records immutable and therefore tamper-resistant, relieving the healthcare sector of the large sums of money it spends due to ransomware attacks.
- This application is beneficial to patients by providing them with granular access controls to manage which providers have access to their medical records.

References

Abrol, Ayushi. “Hyperledger Vs Corda Vs Ethereum: A Detailed Comparison.” *Blockchain Council*, 25 Mar. 2022, www.blockchain-council.org/blockchain/hyperledger-vs-corda-vs-ethereum/.

Celesti, Antonio, et al. “Blockchain-Based Healthcare Workflow for Tele-Medical Laboratory in Federated Hospital IoT Clouds.” Sensors (Basel, Switzerland), 2 May 2020, www.ncbi.nlm.nih.gov/pmc/articles/PMC724908/.

Chen, Chin-Ling, et al. “A Blockchain-Based Secure Inter-Hospital EMR Sharing System.” MDPI, 19 July 2020, www.mdpi.com/2076-3417/10/14/4958.

Crittenden, Camille, et al. “Blockchain in California: A Roadmap.” California Blockchain Working Group, July 2020, www.govops.ca.gov/wp-content/uploads/sites/11/2020/07/BWG-Final-Repot-2020-July1.pdf.

Heston, Thomas. “A Case Study in Blockchain Health Care Innovation.” ResearchGate, Nov. 2017, www.researchgate.net/publication/321478417_A_case_study_in_blockchain_health_care_innovation.

Jamil, Faisal, et al. “A Novel Medical Blockchain Model for Drug Supply Chain Integrity Management in a Smart Hospital.” MDPI, 7 May 2019, www.mdpi.com/2079-9292/8/5/505.

“UK Digital Identity and Attributes Trust Framework - Beta Version.” GOV.UK, 11 Jan. 2023, www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version.