Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2020, 7(8):211-214**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Is Block Chain Secure for Healthcare Interoperability?

Swapna Nadakuditi

Sr IT Business Systems Analyst Florida Blue

Abstract With the exponential growth in healthcare data, there is a greater need for an elevated level of security and privacy. Privacy means having the correct rights to allow or disclose personal information to others. Privacy helps to determine how access to personal patient information is controlled. Healthcare security on the other hand is extremely important to healthcare providers to help safeguard the privacy of patient's health information. This includes managing access control of patient information, the security of patient data from unauthorized users, and the modification and destruction of stored data. The increased adoption of electronic health records, coupled with personal health records and health information exchanges resulted in increased challenges in protecting and safe access to data [1].

The Health Information Technology for Economic and Clinical Health Act (HITECH) was created to promote and expand the adoption of health information technology, specifically, the use of electronic health records (EHRs) by healthcare providers. The HITECH law also proposed the meaningful use of interoperable electronic health records across the health care delivery system to ensure EHR technology is used in a manner of providing secure data exchange between the organizations. Ensuring adequate privacy and security protection for personal health information is one of the principles of meaningful use. This was achieved through financial incentives for adopting EHRs and increased penalties for violations of the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. The HITECH Act also helped to ensure healthcare organizations and their business associates were complying with the HIPAA Privacy and Security Rules were implementing safeguards to keep health information private and confidential [2].

Keywords Blockchain, Health Information Exchange, Interoperability, Client-server, Electronic Health records, Hash, nodes, HIPPA, Application Program Interface (API)

1. Introduction

Interoperability in healthcare is about data exchange between business entities for example, between multiple hospital systems using Health Information Exchange (HIE) for the purpose of improved patient care and is also known as institution driven interoperability. However, the patient's medical data should be allowed to be managed and utilized by patients themselves instead of the hospitals. in which case the health data exchange is patient-mediated and patient-driven. This is called patient-centered interoperability. Currently, healthcare systems use centralized client-server-based architectures in which privacy or security flaws may lead to failures in the system [2].

Interoperability has several potential benefits for healthcare. Primarily, it would improve operational efficiency by decreasing the time spent procuring paper-based medical records from other locations and manually entering the data every time. It also helps in reducing redundancy in clinical interventions such as lab tests etc. thereby reducing cost and finally it always improves the quality of care due to the easy availability of the patient's clinical data. The goal of interoperability is to provide cost-effective and comprehensive patient care.

Few ways to enable Patient-Driven Interoperability is.

- Providing incentives to healthcare organizations for sharing data with patients after every encounter in electronic form via automatic updates.
- Creating a standard, public API for health data for both clinicians and patients. The Meaningful Use Stage 3 Final Rule required certified EHR technology to provide an API through which patients can have access to their EHR data.
- Creating a set of reference documents or procedures on the transfer of patient data to and from patient-controlled data repositories as well as effortless ways to manage the scope of, or revoke, consent.
- Adopting a strong authentication framework to identify patients and allow access and use of their data [3].

2. Current Issue

In recent years healthcare organizations have developed several cloud-based solutions to enable the patient's access to medical data. However, there are a lot of challenges in storing patient records in a cloud-based centralized database as these systems are prone to errors, attacks, and data loss due to a single point of failure. Also, the current client-server or the cloud-based systems face the challenges of system vulnerability, data fragmentation, lack of accountability, security, and privacy

Patient-centered interoperability comes with many challenges, such as governance, data standards, electronic patient-consent, security, and privacy. Hence there is a need for technology that could facilitate the shift to patient-centered interoperability. This is where the technology of blockchain helps significantly. Using blockchain technology the participants in a network would be able to record transactions and share them with other participants connected to the blockchain immediately. One advantage of using blockchain technology in the healthcare industry it can improve interoperability of healthcare databases, providing increased access to patient medical records, device tracking, and systems within the blockchain infrastructure [2].

What is a blockchain?

Blockchain is a chain of an immutable record of transactions or data in the form of blocks linked or chained together by cryptographic signatures, called a hash, stored in shared ledgers, and supported by a network of connected processes called nodes. Thus, with blockchain technology, patients will be able to access their medical data by connecting to any hospital. Blockchain technology allows patients to specify rules for their medical data access, like who can access the data, for how long the data can be accessed, and for what purpose. The blockchain is based on the distributed records which hold information. In other words, a block is a record of new transactions e.g., Patient vitals. When the new block with the transaction is full, it would be added to the previous blocks and can be accessed anytime.

These blocks of transaction records are unchangeable, as each block of data is linked to the previous block by including the previous block's unique hash, which is derived from the block's content. In the event of any unauthorized updates to the content of a block, the block's hash would change, disconnecting it from the subsequent block. This would require the user from having to re-hash every block to link them all together. Since these ledgers are present in multiple locations it would become impossible to modify all the blocks thus making these transactions very secure.

The key aspects of blockchain technology, such as decentralized management, immutable audit trail, robustness, and improved security and privacy resulted in improved medical record management [4].

- Decentralization: The data is shared directly in a distributed ledger without the need for a transitional entity. The network nodes process all the transactions and update the ledger once an agreement is reached between the nodes.
- Transparency: Changes to the network are visible among all the network participants, making the network highly transparent and secure.Transparency: Changes to the network are visible among all the network participants, making the network highly transparent and secure.
- Immutability: The transactions in the blockchain are stored in blocks and using a cryptographic hash algorithm each block in the chain is linked to the earlier blocks. It is difficult to modify the content on the block as it would affect all the blocks in the chain and since the copy of the blocks is replicated in multiple nodes it would be very secure.

- Traceability: The transparent and distributed nature of the blockchain technology in the form of nodes makes it easy for auditing and trace back the transactions. Every update in the ledger can be traced back to its original state thus making the network more secure, and transparent.
- Trustless: Blockchain enables the transactions of data between unknown parties without the need to trust. This distribution among several nodes in the network and updating the ledger via consensus ensures the correctness of transactions in an untrusted environment.

The most important use of blockchain is the patient's access to their data. The primary advantage of blockchain technology is that everyone in the network would see the same information at a given point in time making it a lone source of truth. All the participants in the network will agree about the data in the nodes. The blockchain thus provides transparency by providing a ledger of all the activity on the network which makes it immutable and helps for monitoring and data audits [4].

3. Privacy and Security considerations

3.1 Privacy

Patient privacy is a key factor to consider when implementing blockchain. The organizations must have a plan to mitigate the risks and concerns on how the patient PHI will be gathered, used, distributed, stored, and finally destroyed.

The new regulations like General Data Protection Regulation (GDPR) in addition to HIPAA, make patient privacy a standard when processing any form of PHI [5]

- Individual Access Rights to Data
  An individual's right to access their data is a major privacy consideration. HIPAA makes it mandatory to ensure the patient data is made available to the individual record upon request. HIPAA requires that a covered entity keep an audit log of data disclosure even though it does not require individual consent to share data for permitted purposes such as research. Distributed ledger technology of blockchain would support these requirements. Article 15 Right of Access by the Data Subject ensures the owners can transfer their data from one electronic storage entity to another without restriction from the data manager.
- Individual Right to Erasure
  Due to blockchains immutable properties, it is crucial to ensure that the data is not attributed to a single entity. Article 17 Right to Erasure ("right to be forgotten") of GDPR addresses this issue. Considering these requirements, it is important to understand where and how the data is stored. For entities that are not covered under HIPPA, it is also needed to consider any regulations that would have an impact on data use from a privacy perspective [5].

3.2 Security

Security includes protecting the confidentiality, integrity, and availability (CIA) of sensitive data and systems. It is important to secure the blockchain and each of the nodes and enterprise systems that are connecting to technology.

- Confidentiality
  Ensuring only authorized access to data in shared ledgers, the validity, and consistency of which are maintained by nodes using mechanisms such as consensus. This can be achieved using a multi-layered approach in private blockchains, where all the connected healthcare organizations are trusted. Setting permissions to restrict the data needs to only what is needed to fulfill their role in the network is another way to prevent unauthorized data access in the blockchain. To protect confidentiality and ensure only authorized access data can also be encrypted on the nodes [5].
- Integrity
  Because of the technology's immutable nature, the users can trust that the data on-chain has not been modified or deleted. Updates can be appended to the chain, however ensuring that the data already added to the chain will not be altered, thus ensuring each data point has integrity.
- Availability
  Availability of the blockchain is enhanced through the decentralization of the network in such a way that if one or more nodes fail, the network will still be available, and the nodes are synchronized back

to ensure consistency and validity once they are recovered. However, technology does not protect the availability of each individual node. As with any traditional network, nodes on a blockchain can be protected using load balancing servers, automated failovers, and other safeguards [5].

4. Conclusion

To transform the quality and delivery of care, interoperability should be adopted in a way that meets the patient's needs and is technology agnostic. By making interoperability patient-driven and vendor-neutral, can help patients have secure, safe, and easy access to all relevant patient data, regardless of technology or platforms. A patient-controlled system can support the growth of highly favorable health system outcomes. First, it enables patients to effectively become health information owners by accumulating data in one place thereby creating a full view of information. The patients can then choose to share their data with physicians as needed rather than vice versa. Therefore, true interoperability should be patient-ecosystem-based without any technical barriers.

The move towards patient-centered interoperability comes with challenges around patient consent, governance, security, privacy, and patient engagement. Blockchain technology can address these challenges by creating a platform for the secure exchange of data by reducing complexity, enabling collaboration, and creating secure and immutable information. For this rapidly evolving field, it would be beneficial if agencies like HHS provide guidance and support for the technology to realize its full potential in health care. By establishing policies and guidelines for a blockchain framework and by coordinating with early-adopters and providing incentives for adopting blockchain the healthcare organizations can be motivated to adopt blockchain.

There are opportunities to educate on the advantages of blockchain in healthcare, business values it can provide, its privacy and security implications, and how it can be integrated with the existing legacy systems. While the adoption of blockchain in healthcare is still in the infancy, there is a scope for significant growth given its potential.

References

[1]. T. Herzig and T. Walsh, Implementing Information Security in Healthcare Building a Security Program, HIMSS, 2013.

[2]. W. J. Gordon and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," *Computer and Structural Biotechnology Journal*, vol. 16, pp. 224-230, 2018.

[3]. K. D. Mandl and I. S. Kohane, "Time for a Patient-Driven Health Information Economy?," *New England Journal of Medicine*, vol. 374, pp. 205-208, 2016.

[4]. L. Ismail and S. Zeadally, "Lightweight Blockchain for Healthcare," vol. 7, 2019

[5]. HIMSS, "Blockchain in Healthcare," 2020. [Online]. Available: https://www.himss.org/resources/blockchain-healthcare.

[6]. R. Saripalle, C. Runyan and M. Russell, "Using HL7 FHIR to achieve interoperability in patient health record," *Journal of Biomedical Informatics*, vol. 94, 2019.