Current Cybersecurity Challenges of Applying Blockchain in Healthcare

Nahla F AL Hamad & Dr. Jing-Chiou Liou
Department of Computer Science,
Kean University
1000 Morris Ave.
Union, NJ 07083, USA
hamadn@kean.edu, jliou@kean.edu

***Abstract*— The most significant problems faced in electronic healthcare are data protection, sharing, and interoperability. These problems may be reliable by using Blockchain. With blockchain, transparency and trust can be established in transactional systems by using a peer-to-peer (P2P) distributed ledger technology. This technology enhances security, data exchange, interoperability, integrity, and real-time updating and access when correctly implemented. Blockchain regulates accessibility to the database, and transfers of rights among individuals based on certain situations and it facilitates access to the information of user profiles, the user will have full access to his information and control how his data will be shared. A blockchain would also securely store access control policies, and only the users could change them. This creates an environment of transparency and allows the user to make all decisions as to what data is collected and how the data is shared. However, the most difficult challenges for blockchain healthcare are the data backup and compliance with regulation. There are national and international privacy laws such as HIPAA, EU's General Data Protection Regulation, and the GDPR-like California Consumer Privacy Act. Decentralization in blockchain makes it impossible to have a full data backup.**

Keywords*— (Blockchain, Healthcare, Decentralization, Access control, Regulations, accessibility, Immutable, Distributed, backup)***

I. Introduction

"Blockchain" refers to the way BC stores transaction data in blocks that are linked together to form a "chain." The chain grows as more transactions are processed. A chain of blocks is used to record every entry in your personal ledger, so the care you receive is also recorded. [1]

Blockchain is a peer-to-peer (P2P) distributed ledger technology for a new generation of transactional applications that establishes transparency and trust. Blockchain is the underlying fabric for Bitcoin and is a design pattern consisting of three main components: a distributed network, a shared ledger, and digital transactions [2].

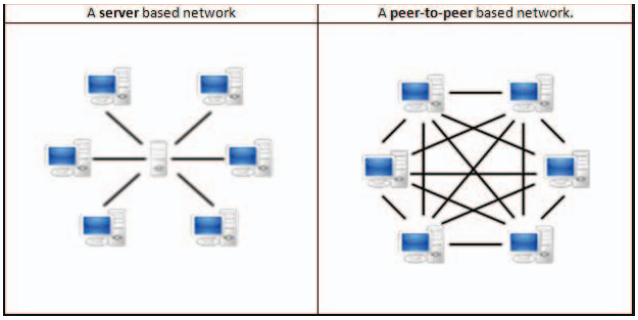

Figure 1:https://coindataflow.com/clue/what-is-blockchain

The most promising applications of blockchain in the health care sector are for identity management, dynamic patient consent, and management of supply chains for medical supplies and pharmaceuticals [3]

This report will discuss the types of blockchains, the benefits, and limitations of blockchain in healthcare, the backup in blockchain, and then the HIPAA and GDPR regulations.

II. Blockchain Elements

A. Smart Contract

A smart contract is a code that activates when certain conditions are met. In the blockchain, there are three types of smart contracts: registrar contracts, patient-provider relationships (PPR), and summary contracts.

B. Distributed ledger technology

The distributed ledger and its immutable record of transactions are accessible to all network participants, minimizing the duplication of effort typically associated with traditional business networks.

2769-5654/22/$31.00 ©2022 IEEE
DOI 10.1109/CSCI58124.2022.00305

Figure 2: https://www.coinreview.com/distributed-ledger-technology/

C. Immutable records

After a transaction has been recorded in the shared ledger, it cannot be changed. If a transaction record includes an error, a new transaction must be added to reverse the error. [13]

III. What are the types of Blockchain?

There are three types of blockchains: public blockchain, private blockchain, and consortium blockchain or hybrid. In a public blockchain, all nodes are accessible and visible to all nodes in the network, a private blockchain is usually managed by a single organization and highly secured and its users have complete anonymity. The hybrid blockchain allows a specific group to join the network and it can be managed by more than one organization, it includes the private and public network characteristics.

To make health care blockchain work, it would have to be public, and it would also have to include technology solutions for three main elements: scalability, data security, and privacy.

	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Access	• Anyone	• Single organization	• Multiple selected organizations
Participants	• Permissionless • Anonymous	• Permissioned • Known identities	• Permissioned • Known identities
Security	• Consensus mechanism • Proof of Work / Proof of Stake	• Pre-approved participants • Voting/multi-party consensus	• Pre-approved participants • Voting/multi-party consensus
Transaction Speed	• Slow	• Lighter and faster	• Lighter and faster

Figure 3: https://coindataflow.com/clue/what-is-blockchain

IV. Advantages, Features, and Limitations of Blockchain

A. Features of blockchain for healthcare domains

There are many features of blockchain that can make existing healthcare systems more efficient. [4]

- *Protection of healthcare data.*
- *Personal health record data management.*
- *Point of care genomics management.*
- *Managing electronic medical record (EMR) data.*
- *Tracking disease and outbreaks.*
- *Interoperable electronic health records.*
- *Decentralization.*
- *Transparency.*

B. The Advantages of the blockchain in healthcare

The following points are the advantages of blockchain in healthcare [5]:

- *Data liquidity: providing the right information at the right time to the right person.*
- *Data immutability: protects the data from any losses. Data cannot be deleted or changed.*
- *Transparency in information auditing.*
- Data aggregation: provides a complete picture of the medical record of a patient for effective medical interventions.
- Digital access rules: rule involves the use of smart contracts for accessing their clinical data stored either on-chain or off-chain.
- Patient identity: storing and accessing information, can be managed by patients through a patient key (public key) based on public key infrastructure.
- Reduces needless overhead expenses.
- The development of further advances in analytics [6]

C. The limitation of the blockchain in healthcare

By overcoming the challenges associated with data security, privacy, sharing, and storage, blockchain has great potential in healthcare. [7]

- Lack of expertise.
- Deployment of blockchain technology in health at a national scale is rare due to the differences in regulations and compliance.

- Blockchains are unsuited for storing large volumes of data, since replication across each network node requires both computational and storage resources. For example, storing full electronic medical records or genetic data records on the blockchain would be inefficient and expensive.
- It is difficult to control data because there is no single data controller since it is network nodes that each hold a copy of the data.
- It is difficult to search for specific terms or information in distributed ledgers. Because of this, they cannot be utilized as information repositories for clinical or research purposes.
- Privacy issues and a lack of robust security are problems that make Bitcoin public blockchain unsuitable for health blockchain that needs privacy and controlled, auditable access.

V. BACKUP IN BLOCKCHAIN

As mentioned before blockchain is gaining the attention of researchers due to its beneficial priorities of decentralization, anonymity, data transparency and traceability. But the development of blockchain is limited due to the limited storage capacity [8].

Blockchain technology is used to ensure the security of edge computing equipment, and edge computing is used to process big data of microgrids.

An integrated blockchain-based microgrid disaster backup scheme is proposed in an edge computing environment to solve the problem that data loss is difficult to recover and to realize distributed data storage and automatic disaster backup technologies.

To overcome the disadvantages of traditional data disaster backup schemes, such as overreliance on the third party, inability to eliminate disaster backup automatically, low security, poor reliability, and inefficiency, a microgrid-based data disaster backup scheme is designed in the edge computing environment, where it is possible to realize a data disaster backup automatically using the Kademlia algorithm. Using the improved PoA, data processing efficiency can be greatly improved, thus resolving the problem of traditional centralized disaster backup, and improving system security [8]

A. Characteristic of blockchain-based microgrid data disaster backup scheme:

- New HE-AES algorithm: With the combination of HE technology and AES, the new HE-AES algorithm improves the encryption speed, as well as resisting the violent cracking of the adversary [8].
- The Kademlia algorithm: It provides distributed storage and disaster recovery of data automatically, which can dramatically reduce routing query speeds compared to other distributed technologies [8].
- The PoA: is used to enable each node to reach consensus and pack the blocks to improve transaction efficiency. Some improvements are made to PoA [8]:
  - The verifiable random function (VRF): It improves the selection of authorized nodes by introducing committee-endorsing mechanisms.
  - The PageRank algorithm and Pareto distribution are used to improve the selection process of leader node.
  - The HotStuff is used in order to establish the framework of finality, which is integrated with the PoA so as to introduce the block finality mechanism to assure the absolute security of the block.

B. Some Pieces of Research and Proposals

- Bae and chin proposed an automatic recovery system using blockchain, assuming that the copy file was created and managed as a block successfully, If the copy was destroyed, the disaster recovery system would check the authenticity of the copy file by pointing to the blockchain and then continue to recover, but due to the PoW adopted in the system, transaction processing efficiency was low, which was not suitable for real-world scenarios [8].
- Su et al. proposed a secure content caching scheme to secure mobile social networks from disasters using fog computing, which included the use of scrambling and partitioning methods to encrypt content, the delivery and storage of encrypted content in multiple clouds servers, and the use of an auction game model to identify the optimal cloud servers. Edge nodes and selected servers can provide the greatest utility. In this scheme, the plaintext was only scrambled without any encryption or hiding, so its security needed to be improved [8].

C. blockchain-based microgrid data disaster backup scheme Framework

The scheme is divided into 4 layers [8]:

- Data Layer: this layer contains microgrid nodes that are the source of data.
- Supervision Layer: this layer contains the registration center that is responsible for generating and distributing passwords and keys for microgrid and edge servers during the initialization.
- Storage Layer: this layer contains the edge servers used to clean, compress, and encrypt the data. Then, the encrypted data block is stored in the edge server.
- Consensus layer: this Layer contains blockchain which is mainly responsible for receiving and storing the effective information uploaded by the edge server.

VI. Regulation and Compliance

The safety and privacy of sensitive health records are governed by several regional and international regulations. Among these regulations are the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR).

Further, compliance with safety standards will increase the trust that components will operate safely under predetermined conditions. [9]

A. Health IT Legislation in U.S

- HIPAA (Health Insurance Portability and Accountability Act)1996: Provides protection for workers and their families when they change jobs, establishes national standards for electronic health care transactions, and creates national identifiers for employers, insurers, and providers. It also describes how to use and disclose protected information, and who is covered by the HIPAA privacy protections. HIPAA is now most associated with the privacy of patient healthcare information. HIPAA Administrative Simplification Rules are administered and enforced by Medicare & Medicaid Services, including Transactions and Code Set Standards, Employer Identifier Standards, and National Provider Identifier Standards. [10] . PHI, according to HIPAA, refers to information that pertains to the mental or physical health of a person. In order to provide PHI with security and privacy, HIPAA covers protected organizations and associations, and protected organizations and business associates are prohibited from disclosing or using PHI without prior consent from the patient unless an exception applies. [11]
- MACRA (Medicare Access and CHIP Reauthorization Act)2015: Implemented the Quality Payment Program (QPP) in place of the Sustainable Growth Rate formula. It describes how doctors will be paid and cost controls for Medicare.
- HITECH (Health Information Technology for Economic and Clinical Health)2009: It empowers HHS to promote health information technology, including electronic health records and private and secure electronic health information exchanges, with the aim of improving health care quality, safety, and efficiency. The HITECH Act can be considered the enforcement wing of HIPAA; because healthcare providers have increasingly become targets of hackers since healthcare records cannot be canceled, changed, or refunded after a breach. The regulations require patients to be notified if their information has been accessed or used without their permission. PHI (protected health information) can only be shared securely. [12]
- FDASIA (Food and Drug Administration Safety and Innovation Act)2012: Ensures that, in consultation with ONC, the Chairman of the Federal Communications Commission, and the Commissioner of the FDA, the Secretary of Health and Human Services develops a report that provides recommendations on an appropriate risk-based regulatory framework for health IT, including medical mobile applications, to promote innovation, protect patient safety, and prevent regulatory duplication. [10]
- Affordable Care Act of 2010: Provides new consumer protections, increases access to health care and improves quality and costs. [10]

B. Health IT Legislation in E.U.

GDPR has been in place since 25 May 2018, GDPR became E.U law and had to be followed by all EU countries. In addition to storing, exchanging, and using health data, this integration of EU law covers all personal information. The handling of health data by E.U citizens is likely to cost and benefit healthcare practitioners and health analysts.

According to GDPR, individuals have many significant privileges, such as [11]:

- Right to know what data is being collected.
- Access to information is a fundamental right.
- The right to portability of data.
- The right to object to the storage.
- The right to correct incorrect data.
- When data is no longer preserved, the right to forgetting is highly controversial (especially in the context of free speech).

The collection, use, and transmission of health and scientific data are becoming increasingly regulated, strengthening the DPD's patchwork of rules. It is typical for specific rules to be complex and burdensome compared to previous laws. Health and genetic data, deemed "sensitive," require specific guidelines and conditions to be followed before they can be processed. The condition included the following: "Explicit' consent was granted if:

- Providing the consent of a patient unable to give consent, such as an unconscious patient.
- Whenever it is necessary to offer health care to patients as if one doctor needs data from another doctor.
- Protection against cross-border health threats or preserving health safety are just some examples of health that needs to be addressed.

C. Requirements for HIPAA and the GDPR compliance solution

The HIPAA prohibits the collection and use of health data for research, medical or any other related purpose in the US, while the GDPR mandates the protection of personal information in the EU. As well, organizations that transfer U.S.

health-related data to the European Union must comply with both rules.

Main functional differences between HIPAA and GDPR [11]:

- GDPR consent provisions are not guaranteed to be complied with by the Institutional Review Board (IRB). IRB approvals are handled separately. In spite of this, GDPR demands will not be waived if an institution in the E.U. processes consent-based health data and guarantees that informed consent records in the U.S. are compliant.
- In addition to GDPR access, corrections, and erasure rights, EU GDPR data subjects have much broader rights than US Consent agreements. These rights should be familiarized by organizations that collect or process European Union data. It is also possible that the approval and compliance of the US IRB are insufficient.
- Almost all aspects of the GDPR one-stop shopping law are simplified. There are also several conditions that cannot be ignored, including the name of a data protection authority delegate in the chosen E.U. country.
- Data transfer from members of the E.U. to U.S. members is often the most complicated. In every international health data project design process, this is a different problem that must be tackled since the guidelines are detailed and usually uncompromising.

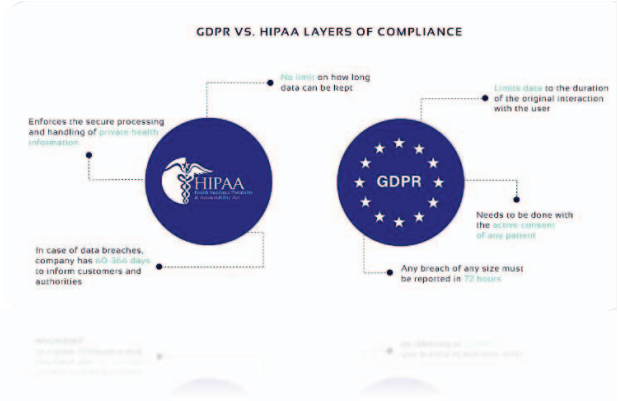

Figure 4: https://light-it.net/blog/things-you-should-know-before-you-create-telemedicine-app/

D. Proposed solutions for healthcare compliance with HIPAA and GDPR

In addition to pseudonymization and encryption, HIPAA and GDPR require effective technical measures to protect health information. These are difficult to implement correctly, and extensive development resources are required. [11]

- Organizations are responsible for technological requirements. It is necessary to take further measures, such as encrypting records and auditing them. AWS, Azure, etc. do not require any additional security. Professional development teams are required to implement these requirements, however, since they are difficult to implement.
- Even though attorneys can handle administrative requirements, they do not have the capability of completing complex documents such as DPIAs and BAAs.
- Firewalls, load balancers, etc., are typically managed by the organization's cloud provider.

VII. Conclusion

A blockchain in healthcare removes the middleman, enhances security, improves quality of care, reduces manual errors, and decentralizes patient data. In a blockchain, there is no central authority and all information stored on it is transparent and immutable. As a result of blockchain healthcare, patients will not have to fill out numerous forms when they change hospitals, since their new physicians will be able to view all their information on the blockchain network.

Each record on a blockchain is called a "block". Each block contains a cryptographic hash of the previous block.

With blockchain technology, healthcare inefficiencies and waste can be significantly reduced.

Almost every day, we are using smartphone apps and devices to collect our critical health data. The data is already shared with a variety of organizations, but it isn't secure. However, blockchain technology can be used to transfer data between healthcare providers in a safe and secure way.

Although blockchain provides more integrity, traceability, and security, data backup and compliance with regulation are the main challenges for healthcare blockchain.

Decentralization, anonymity, data transparency, and traceability are some of the characteristics of blockchain technology that attract experts and scholars. But the limited capacity for storage will be a challenge.

With edge computing and blockchain technology combined, edge computing is used to process big data of microgrids and reduce data scale, while blockchain technology ensures the security of edge computing equipment. Blockchain-based microgrid data disaster backup schemes can eliminate the difficulty of recovering data losses and realize automatic disaster recovery.

REFERENCES.

[1] K. G. E. a. S. M. M. Matthew N. O. Sadiku, "Block chain Technology in Healthcare," *International Journal of Advances in Scientific Research and Engineering (ijasre),* 2018.

[2] L. Linn and K. Martha , "Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research," ONC/NIST Use of blockchain of healthcare and research workshop, Gaithersburg, MD, USA, 2016.

[3] OECD, "Opportunities and Challenges of Blockchain Technologies in Healthcare," OECD, Europe, 2020.

[4] I. Y. •. K. S. •. R. J. •. Y. Al-Hammadi1, "Blockchain for healthcare data management: opportunities, challenges, and future recommendations," *Neural Comput & Applic ,* 2020.

[5] Y. Maleh, M. Shojafar, M. Alazab and I. Romdhani, Blockchain for Cybersecurity and privacy Architectures,Challenges and Applications, Oxon: CRC Press, 2020.

[6] "Blockchain for Healthcare," HHS, U.S., 2021.

[7] S. Khezr, M. Moniruzzaman, A. Yassine and R. Benlamri, "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research," *MDPI,* 2019.

[8] L. Zhan, Y. Cao, G. Zhang and C. Zheng, "A Blockchain-Based Microgrid Data Disaster Backup Scheme in Edge Computing," *Security and Communication Networks,* 2021.

[9] P. Kubben, M. Dumontier and A. Dekker, Fundamentals of Clinical Data Science, Maastricht, Limburg, 2019.

[10] "Health IT Legislation," 5 July 2022. [Online]. Available: https://www.healthit.gov/topic/laws-regulation-and-policy/health-it-legislation.

[11] M. Shuaib, S. Alam, M. S. Alam and S. M. Nasir, "Compliance with HIPAA and GDPR in blockchain-based electronic health," *Materials Today: Proceedings,* pp. 1-6, 2021.

[12] "5 Important Regulations in United States Healthcare," 5 July 2022. [Online]. Available: https://online.maryville.edu/blog/5-important-regulations-in-united-states-healthcare/.

[13] IBM, "Blockchain success starts here," [Online]. Available: https://www.ibm.com/topics/what-is-blockchain.

[14] M. Miliard, "As blockchain proves its worth for healthcare, regulatory questions remain," 2018. [Online]. Available: shorturl.at/tCQVY.