An Overview Of Blockchain In Healthcare

Pooja Jadon, Assistant Professor
Department of Computer Science and Engineering, Vivekananda Global University, Jaipur
Email Id- pooja.jadon@vgu.ac.in

ABSTRACT: In the past several years, the health-care industry has been more interested in blockchain technology. The value proposition for blockchain technology in the health-care industry is to securely exchange sensitive patient data across health-care organizations while also empowering individuals. Patients may take an active part in creating and updating their own health data thanks to blockchain technology. Is blockchain technology, however, truly the panacea it seems to be we want to get a better understanding of the advantages and difficulties of blockchain technology in the health-care industry through this study. We explore the potential of blockchain technology in health care for innovation and security. Furthermore, we demonstrate that further use cases are required to guarantee safe data exchange in the health-care industry. In our view, blockchain technology will not address the problems that the health-care industry is facing; in fact, it may create more problems than it solves.

KEYWORDS: Bloclchain, Consequences, Healthcare, Patient, Transaction.

1. INTRODUCTION

Blockchain technology is expected to transform businesses and sectors beyond its initial use as the peer-to-peer payment system Bitcoin. The banking sector, the supply chain industry, the payments industry, and e-commerce have all seen significant use of blockchain technology. Blockchain technology has the potential to improve the health-care industry by making health-care information systems more patient-centric and enabling safe and efficient health data exchange[1]. A slew of studies have suggested different possible use cases for blockchain in health care, however the overwhelming majority of those use cases have yet to be realized[2].

Patient-managed health records, improved insurance claim processes, improved health care research, and advanced medical records shared among patients and health care providers are some of the common use cases that benefit from blockchain-based solutions for a patient-centric health care information system. Despite the appropriateness of blockchain solutions for issues and innovation requirements in health care information systems, full implementation is difficult to regulate. Even though certain solutions have proven viable in reality, they need data size and operational cost reductions, as well as improved privacy and security protection of personal information[3].

Interoperability and scalability problems are also hindrances to fully adopting blockchain-enabled patient-centric electronic medical records. The absence of standards across different blockchain-based systems reveals interoperability problems. However, suggestions to remedy such problems have been made[4]. Scalability problems emerge as a result of the large amount of clinical data, since blockchain-based systems have data size limits[5]. Patient involvement seems to be an advantage of blockchain-based health-care systems; however, this is unlikely to be the case for all kinds of patients, since not all patients are interested in controlling their own data. Individual rights guaranteed by the General Data Protection Regulation (GDPR) have not been properly evaluated for blockchain-based solutions.

Patients, health care professionals, and researchers are all affected by the opportunities, obstacles, and concerns described above. In addition, the legal, security, and privacy concerns should be investigated further[6]. This may lead to various workarounds to make the blockchain architecture GDPR-compliant, although nothing substantial has yet been developed[7]. We hope to discuss the innovation and security implications of blockchain in the health-care sector in this viewpoint article. Because there are already extensive research studies on blockchain in health care, we did not try to perform a full literature study on the subject. Rather, we provide our point of view on the consequences of blockchain for the health-care industry, backed up with research[7].

As a result, we want to find an answer to our study question: What consequences could blockchain technology have for the health-care industry. First, we'll go through the basics of blockchain technology.

Second, we go through the ramifications of using blockchain to innovate in health care. Finally, we go through the security concerns of blockchain in the healthcare industry[8]. Finally, we wrap up our debate and put this paper to rest. Blockchain technology is characterized as a disruptive breakthrough that offers possibilities and difficulties to a variety of businesses and sectors , and it merits more investigation. The question of whether blockchain or Bitcoin originated first is still being debated . The underlying technology, blockchain, has a wider set of capabilities and features. Bitcoin is just a trading program that incorporates blockchain features. When Stuart Haber and W Scott Stornetta developed a framework for a "timestamping digital document" to generate hash values that uniquely identify documents and store them in certificates with a timestamp, they were the first to introduce the concept of blockchain[9].

A data structure connects these documents to the hashes of earlier records. Nakamoto used Haber and Stornetta's architecture to create the initial Bitcoin peer-to-peer payment system, which is based on timestamped blocks of transactions that are chained using previous blocks' hash values. After then, Bitcoin became well-known as a way to trade cryptocurrency. Blockchain, according to Swan, is a decentralized, transparent ledger containing transaction data. A blockchain is made up of a collection of data blocks, each of which includes information on numerous transactions (ie, transactions list, timestamp, nonce, hashes of the transactions and their root hash or block hash, and the hash of the previous block). The distributed ledger creates a full transaction history book when additional blocks are added to the chain . Before adding new transactions to the ledger, several participants use the consensus method to verify the transaction and the block. Transactions stay in the block for a certain amount of time until the consensus process is completed[10].

The transaction block is then recorded in the ledger, where the data cannot be altered. If a block's hash is changed, the block loses its validity, making future blocks invalid as well, necessitating the verification of the block after recalculating its hash and the hashes of following blocks. The two most common blockchain deployment models are public permissionless and private permissioned blockchains. Public permissionless blockchains are open and decentralized, with anybody having the ability to join and leave the network at any moment as a reader or writer (e.g, Bitcoin). There is no central authority to oversee the network, and no one owns or manages it. Private permissioned blockchains only allow a certain group of readers and authors to participate (eg, Hyperledger). Individuals with the right to read and write operations are assigned by the network's central authority. Several definitions of blockchain primarily relate to the properties of public permissionless blockchains, such as absolute immutability, anonymity, decentralization in consensus mechanism operation, and openness.

Private permissioned blockchains, which are controlled by a central trusted authority that controls the consensus process and in which the identities of participants are specified and access rights are limited, are not described in the definitions. Blockchain technology is billed as a "accelerating engine of innovation" with a slew of advantages . However, a lengthy list of security risks refutes assertions that blockchains are tamperproof and provide robust security. Blockchains are said to be immutable and unhackable, although this claim has been debunked. Furthermore, blockchains are energy-intensive, resulting in significant expenses (e.g., network performance issues). This raises the question of whether the advantages and promises offered by blockchain can be taken for granted, or if they will represent a danger to innovation and security goals. As a result, concerns about the advantages and dangers of blockchains remain unanswered in practice and research, including whether blockchain is a radical or gradual revolution in nature.

1.1 Implications of Blockchain Innovation in Health Care:

Blockchain is a disruptive innovation that has the potential to enhance patient care by using the capabilities of health care information systems; nevertheless, it has significant regulatory, financial, and operational consequences. Private permissioned blockchains are an appropriate alternative for dealing with sensitive patient data in the health care industry. This kind of blockchain implementation has positive implications for blockchain's usage in health care. Patient-managed medical records, improved insurance claim processes, accelerated medical research with shared anonymous patient data, and an advanced health data ledger maintaining clinical transaction logs, pharmaceutical supply chains, and consent recording are some of the use cases suggested by researchers for blockchain in health care.

Despite its significance, research on blockchain's GDPR compliance is limited. Due to the central authority managing the network and access to personal data, private permissioned blockchains have concerns for GDPR. In the case of using patient data to assist health care researchers, a pseudonymization technique is required to protect patients' sensitive data, which could lead to reidentification (i.e., linking the pseudonym code or metadata to the patient's health data), which would be in violation of GDPR. This necessitates a thorough examination of the use case and the blockchain-based health information system's architecture. Because blockchains are immutable, it is impossible to remove a block. As a result, blockchain fails to meet the GDPR requirement that data subjects have the right to request the deletion of their data, including health-related data.

The patient data may be kept off-chain and the pseudonym codes might be stored on-chain. However, even after removing the patient data that was stored off-chain, the pseudonym code and any transaction records on the patient data that is kept on-chain would still remain. A proof-of-concept prototype for a "forgetting blockchain" was suggested to erase outdated data from private permissioned blockchains in order to reverse the immutability of blockchain; nevertheless, the prototype still has constraints to solve. Blockchain, according to Beck and Müller-Bloch, is a fundamental innovation that outdates the traditional distributed systems approach by virtue of its design and features. As a result, radical innovations are difficult to execute and bring with them more complicated problems that need organizational preparedness as well as the upgrading of outdated organizational knowledge and IT infrastructure.

This has financial consequences for the use of blockchain technology in the health-carindustry; although it has the potential to enhance the quality of medical services, it may also generate financial risks. Computational overhead, lack of interoperability and standardization, privacy issues, and ambiguity regarding who is accountable for the expense of technology installation and who benefits from it are the main obstacles confronting the adoption of blockchain in health care.The immaturity of the technology itself, inadequate skills to comprehend and execute it, a lack of buy-in, and a lack of a clear return on investment are all barriers to blockchain adoption in the health care industry.

The lack of buy-in may be traced back to blockchain's unfamiliarity, medical professionals' unfavorable views about its usage, and the fact that not all patients are interested in controlling their health data. According to Beck and Müller-Bloch, three skills are required to manage a radical innovation using blockchain in order to reap its benefits: discovery, incubation, and acceleration. The term "discovery" refers to the process of identifying and articulating blockchain possibilities as well as the formation of research communities. Incubation entails creating blockchain use cases and putting them to the test (ie, proof of concept). Proposing a blockchain implementation and investing in the development of fully functional blockchain logic and infrastructure are both examples of acceleration. The goal of blockchain proof of concept is to mimic real-world circumstances in order to assess the viability of blockchain in health care and solve its problems.

Even though the necessary enhancements have been tested and shown to be effective, they come at the cost of other critical elements of the health information system. Although a proof of concept for a blockchain-based patient-centric information exchange between patients and providers has shown encouraging results, the real-world deployment is anticipated to provide different outcomes. Due to the dynamic regeneration of smart contracts, using blockchain to enhance health data sharing and patient involvement may come at the cost of performance. Furthermore, the size of the experimental files will never be the same as the amount of the patient data. One of the most significant concerns for the viability of blockchain solutions for health care is data size.

1.2 Blockchain's Health-Care Security Consequences:

Private permissioned blockchain implementation is said to provide the greatest advantages for health care applications, but it also poses security concerns. Private permissioned blockchains are restricted to trusted and specified participants, and the rights to read and write activities on the blockchain are managed by a central authority. This feature adds to the level of control by ensuring that only authorized users may access or write to the patient data. This has a beneficial impact on the data's secrecy and integrity. Immutability also allows for the monitoring of patient-generated data for medical research, transactions on insurance claim procedures to identify fraud, and pharmaceutical supply chains to ensure quality. The availability of audit trails and progress tracing may also be enabled via a private permissioned blockchain. Smart contracts allow patients to provide authorization and permission for researchers to access their health data when utilizing patient-generated health data for research purposes. Data integrity, on the other hand, may be jeopardized since the patient data input point, which is the patient's device, can be impersonated. Sharing patient health data with researchers puts the patient's privacy at risk; even if the data is pseudonymized, reidentification is possible. However, efforts to improve patient privacy in blockchain settings and build blockchain features for privacy are still in the early stages of development, and there is no assurance that privacy will be preserved. A 51 percent attack is most likely to affect private permissioned blockchains . This occurs when an attacker compromises the central trustworthy node; since transaction validation is centralized, the attacker obtains the ability to control the network's computing capacity, allowing a transaction to occur twice. As a result, the transaction data's integrity is compromised, and the network's resources are depleted. This has severe consequences for data integrity and service availability, both of which are essential for health-care applications. For the aim of avoiding distributed denial-of-service (DDoS) attacks, private permissioned blockchains have restrictions in storing patient data alongside transaction data. This is a problem since the amount of patient health data is increasing with time. The growing amount of patient data would necessitate addressing the data size restriction in private blockchain, exposing the network to DDoS assaults. Furthermore, verifying a big data block uses a lot of electricity and incurs additional operating expenses. In any scenario, the availability of services, which is essential for health care, would be jeopardized. The security of patient health data using blockchain technology is currently in the proof-of-concept stage, and confidentiality and privacy cannot be guaranteed at this time. The efforts to address blockchain security and privacy in health care seem to be at the cost of other key aspects of blockchain technology or the requirements of the health care industry.

2.DISCUSSION

We looked at the many innovation and security implications of utilizing blockchain technology in the health care industry in our perspective paper. As a result, we return to our original study question: What consequences could blockchain technology have for the health-care industry Although blockchain technology is not new, research into the possibility of using it in the health-care industry is still in its early stages. Innovating with blockchain in health care is now at the proof-of-concept stage. Blockchain is a technical advancement that has both advantages and disadvantages. Blockchain is anticipated to improve the health-care industry by empowering patients and improving immutability and traceability. Sharing large quantities of patient health data among interested organizations (interoperability), regulatory compliance (e.g., GDPR), data confidentiality, data integrity, privacy, and data and service availability are all requirements in the health care industry.

The capacity to store and handle large quantities of patient health data, ensure privacy, and reduce operational costs are all requirements for utilizing blockchain in health care. Customizing private permissioned blockchain solutions to meet the requirements of the health-care industry may include altering blockchain technology's features or manipulating the health-care industry's needs. This is a well-known trade-off strategy used in proof-of-concept blockchain-based health-care systems. This trade-off entails making a choice between two desired but conflicting characteristics. For example, meeting GDPR standards necessitates exploiting blockchain's immutability. Furthermore, blockchain's block size restriction is designed to minimize performance cost and avoid DDoS assaults. This, however, limits the scalability required to handle the massive amounts of patient health data, and managing such large amounts of data is challenging. However, if the blockchain is built to handle huge amounts of data, it would incur additional operational expenses owing to the performance overhead, as well as expose the network to DDoS assaults.

3. CONCLUSION

From the time it was first introduced to the public, blockchain technology has progressed. Bitcoin has evolved into a general-purpose technology with applications in a variety of fields, including healthcare. To gain a better understanding of the current state of blockchain technology's application in healthcare, We carried out a systematic review in which we used the to create a map of all relevant research. Process of systematic mapping research . The study's specific goals were to find out what was going on in the world. Use cases for blockchain technology in healthcare, as well as examples of applications that have been created for these use cases, the blockchain-based healthcare apps' difficulties and limits, the existing methods for creating these applications, as well as topics for future study We found 65 papers using our search and paper selection protocol, which we analyzed to find answers to our questions. questions for research.

REFERENCES:

[1] A. Gantait Joy Patra Ayan Mukherjee, "Implementing blockchain for cognitive IoT applications, Part 1 Integrate device data with smart contracts in IBM Blockchain," *IBM Dev.*, 2017.

[2] M. Bhat and S. Vijayal, "A probabilistic analysis on crypto-currencies based on blockchain," 2018, doi: 10.1109/ICNGCIS.2017.37.

[3] R. Asija and R. Nallusamy, "A Survey on Security and Privacy of Healthcare Data," 2014, doi: 10.5176/2251-3833_ghc14.29.

[4] N. Kristeva and S. Stoyanov, "Healthcare system and healthcare reform," *Bulgarian Medicine*. 2002.

[5] T. Jones, M. DeMore, L. L. Cohen, C. O'Connell, and D. Jones, "Childhood healthcare experience, healthcare attitudes, and optimism as predictors of adolescents' healthcare behavior," *J. Clin. Psychol. Med. Settings*, 2008, doi: 10.1007/s10880-008-9126-7.

[6] D. Von Lubitz and N. Wickramasinghe, "Healthcare and technology: The doctrine of networkcentric healthcare," *International Journal of Electronic Healthcare*. 2006, doi: 10.1504/ijeh.2006.010440.

[7] A. Muluken, G. Haimanot, and M. Mesafint, "Healthcare waste management practices among healthcare workers in healthcare facilities of Gondar town, Northwest Ethiopia," *Heal. Sci. J.*, 2013.

[8] R. D. Caytiles and S. Park, "u-healthcare: The next healthcare service paradigm," *Int. J. Bio-Science Bio-Technology*, 2012.

[9] B. Bronkhorst, "How 'healthy' are healthcare organizations? Exploring employee healthcare utilization rates among Dutch healthcare organizations," *Heal. Serv. Manag. Res.*, 2017, doi: 10.1177/0951484817715031.

[10] N. F. Habidin, N. A. Shazali, M. I. Salleh, Z. Zainol, N. S. Hudin, and W. S. W. Mustaffa, "A review of supply chain innovation and healthcare performance in healthcare industry," *International Journal of Pharmaceutical Sciences Review and Research*. 2015.