Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-002
www.ardjournal.com | DOI:

BLOCKCHAIN-ENABLED PATIENT-CENTERED HEALTHCARE DATA MANAGEMENT SYSTEM

B. VEENA, ***Assistant Professor,***
Department of CSE(AI&ML),
SUMATHI REDDY INSTITUTE OF TECHNOLOGY FOR WOMEN, TELANGANA.

ABSTRACT: Blockchains are a safe way to store and send data because they are independent and permanent. Every link in the chain has its own information, and each one is important to the whole. As a result, the network is run by people who are directly involved with distributing and maintaining data, not by a third party. Blockchain technology is being used by pharmaceutical businesses to store and share data from electronic medical records and clinical trials. There are also mobile health apps and monitoring tools that use it. It could also be used for "management of insurance information." There isn't enough research on blockchain technology in healthcare right now. There will likely be big changes in the near future. The distributed ledger architecture of blockchain makes data storage safer and makes it easier to quickly get medical information. This shows that, unlike the usual way of doing things, people are responsible for their own health care.

Keywords: *Blockchain; Data Security and Confidentiality; E-health; Electronic Health Records; Healthcare Service Innovation and IT.*

1. INTRODUCTION

Data ownership and privacy are important topics that need serious thought. At the moment, there is no guarantee that patient privacy will be protected when dealing with medical data. However, there are significant negative effects associated with data exposures. Multiple data invasions resulted in the compromising of 13 million medical information in 2018, according to allegations filed with the Department of Health and Human Services' Office for Civil Rights. The average cost of a data attack in the US is $7.91 million, according to a recent assessment by the Ponemon Institute on behalf of IBM Security. The Ponemon Institute reports that 2018 saw the greatest per capita healthcare spending. People might not have complete control over their own health data. As customized care and cutting-edge technologies proliferate, the problem will worsen.

Similar cryptographic methods share a set of unchangeable elements in every case. Figure 1 shows how a blockchain system works, using the original Bitcoin as an example. Contractual documents, administrative documents, and electronic funds are just a few examples of the types of information that might be included in a consumer-initiated transaction. We can verify the user's identity and the legitimacy of the transaction by using their private and public keys. Multiplying the private key by an elliptic curve yields the public key in a unidirectional mathematical process. This feature makes it possible for outside parties to confirm its legitimacy. Every partner in the network is then sent a notification about the trade. There is a cap on how many transactions each miner may make in a block.

Miners are now vying with one another to decide which transaction hash in their block will be accepted as authentic. Every miner is a node, but not all nodes are miners. This method entails methodically comparing several output sequences to a predetermined set of standards

CC BY NC

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-001
www.ardjournal.com | DOI:

until one meets all the requirements. After the first miner successfully submits their block to the network, the transaction is considered complete. The next cycle starts right away (Figure 1). If a block is changed after it has been added to the chain, all following blocks must be reprocessed, which could be resource-intensive. Since data is dispersed among several nodes, an antagonistic user cannot access the system. This presents a different approach to improving blockchain security. Because of its basic working principles, blockchain is the best tool for monitoring medical data. The healthcare sector has just begun implementing blockchain, highlighting the need for more study.

It is gradually getting easier to access. A blockchain-powered healthcare testing project has been launched by consulting company Booz Allen Hamilton (Cyran). Numerous mobile applications and Electronic Medical Record (EMR) systems have been created.

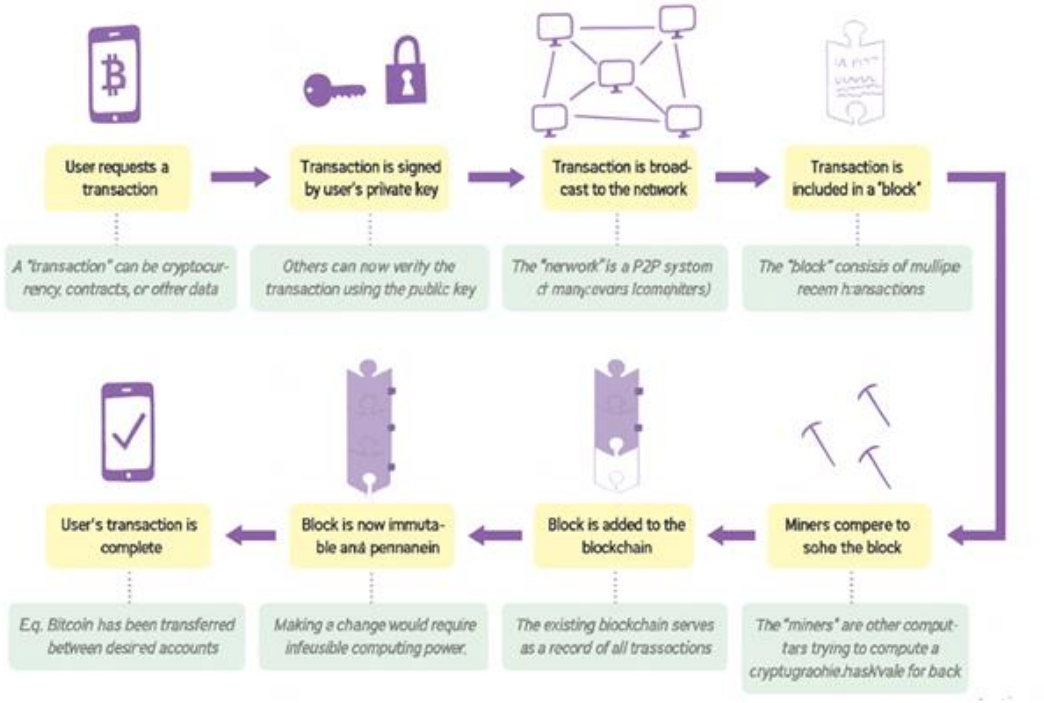

Figure 1: Dissection of how a blockchain system works.

2. MOBILE HEALTH AND REMOTE MONITORING

In contemporary healthcare, this is the most crucial factor. These tools will function better and protect people safer if bitcoin is added. A smartphone app designed to support cognitive behavioral therapy for insomnia was created and tested by a team of professionals. The app stores patient medical data on the blockchain. Because of the way blockchain technology operates, researchers have demonstrated that the network's electronic medical records (EMRs) are secure and impenetrable. The patient had access to their own private data. Recording information and sending it to doctors from any location is made simple by this app. Patients may be able to concentrate more on their overall health and well-being when they are in control of their own care.

A new smartphone app called Healthcare Data Gateway (HGD) was created to make managing patient data simpler. The program handles data using a standard Indicator-Centric Schema (ICS) and a secure Multi-Party Computing (MPC) infrastructure. Private health information can now be accessed by third parties without endangering patients or requiring physical access. This application consists of three primary components: data management,

CC BY NC

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-001
www.ardjournal.com | DOI:

data use, and data storage. They collaborate to ensure that the program functions properly and that the data is secure. The use of blockchain technology to safeguard smart contracts is comparable to the use of security equipment.

Smart contracts monitor events and ensure that everything that occurs on the blockchain is authentic. A worldwide blockchain based on the Ethereum platform has been developed to facilitate tracking from a distance. Using this private blockchain, sensors can transmit data to smart devices that monitor transactions using smart contracts. Patients and healthcare professionals can receive critical messages instantly thanks to smart contracts. This ensures the security of real-time patient tracking. Patients can take control of their own health and well-being with the assistance of medical professionals who are available at all times to answer inquiries and offer guidance. It is crucial to ensure the safety of those receiving home care. Because patient medical information is sensitive and private, mobile healthcare storage is unsafe. Malware on mobile devices has caused significant harm to the blockchain system in the past. Therefore, if health data is stored on the blockchain that enables mobile apps, it must be totally secure. The most hazardous kind of mobile malware, root assaults, was examined in relation to blockchain technology.

The blockchain on which mobile apps are based needs to be totally secure before it can be used to store health data. The most hazardous kind of mobile malware is root assaults, and a study examined blockchain technology. By gaining access to a patient's PKI private key through root attacks, hackers can gain access to blockchain systems.

Because it allows hackers to obtain the patient's PKI private key, a root attack is a vulnerability in blockchain systems that allows them to access private patient data stored on the blockchain. This work used the biologically inspired approach of Practical Swarm Optimization (PSO) to identify critical errors and useful speedups that enhance machine learning efficiency. Finding previously undiscovered root bugs and learning about novel malware variants were their objectives. 93% of root assaults were discovered by Logitboost. Logitboost is capable of detecting root attacks, according to researchers studying the Root Exploit Detection System (RODS). Further research is required to confirm that blockchain can protect patient data, particularly in the areas of remote monitoring and mobile health security.

3. ACCESSING AND SHARING HEALTH DATA

Only one "B" has the ability to display the user's data. Sharing and reviewing medical records is made simple by blockchain technology. It could be more difficult to acquire crucial medical knowledge if there are many healthcare providers. Blockchain technology makes it safe and simple for people to examine all of their medical and other records. Numerous blockchain-based solutions are available for maintaining well-organized and accessible medical records. Med Block is a blockchain-based information management system that facilitates the retrieval and storage of digital medical records. The application uses a sophisticated consensus method to prevent the network from becoming overloaded. The network may find it more difficult to manage new technologies like blockchain. All of the instruments in the Medical Data Pervasion System (DPS) are now in use. The DPS and the government both employ the same security techniques and technologies to protect data. A functioning DPS prototype has been created on the Ethereum network.

CC BY NC

Advanced Research and Development Journal
ISSN: Applied | Volume 1 Issue 1 | October-December 2025 | Inaugural Edition | ARD-001
www.ardjournal.com | DOI:

The global PHR system combines data from numerous sources into blockchain blocks. Now, all patient health information (PHR) is accessible from one convenient spot. By obtaining the most current encrypted block in the chain, the patient can access their private medical records. A patient's therapy would be more effective if all of their medical records were in one location. The C-AB-/IB-ES EHR system was made feasible by the partnership with omniPHR. The method uses encryption and signatures based on names and other data. Blockchain applications that require your name to be verified in order to function are listed by the Ethereum Foundation (2018). Decentralized cloud storage solutions, such as Ethereum Swarm, which can manage more data than blockchains, are used to protect medical information. Ethereum Swarm is an autonomous storage system integrated into the Ethereum web3 platform. The decoder key and a distinct swarm hash for every patient's medical file comprise the root component. Only those with knowledge of the root component reference can access the information. Key components are securely stored in blockchain smart contracts and are only visible in specific situations.

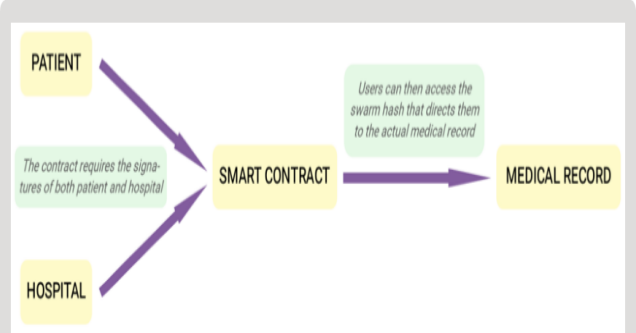

Figure 2: Overview of a proposed blockchain healthcare model.

Contracts with multiple signatures can specify who owns and has access to shared data. In order to use their private keys to verify that a transaction is authentic, many users, such as the patient and the hospital, must communicate with one another. Patients can view their medical records at any time, but they cannot be altered without the hospital's consent. Since the number from the previous entry might have changed, we additionally include the date of the most recent entry. Each time data is accessed, a new swarm hash must be created. The swarm hash is promptly updated when data is modified. If they are granted the proper authority, they can be fairly restrained. This design provides a multisig solution for data ownership and viewing, in addition to the security and immutability inherent in blockchain technology.

5. ADDRESSED CONCERNS

Blockchain systems are susceptible to the 51% attack, also known as the majority attack or the double-spend attack (Yli-Huumo, Ko, Choi, Park, & Smolander, 2016). More than half of the network's mining hash rate could be controlled by one or more miners. They can now terminate any agreements that are still in force or cancel any arrangements that have already been made. The longest chain is the only one that is "acceptable" from this perspective. A malicious user can increase the network's block production rate since they have more processing power. Consequently, the network is forced to employ the chain that the criminal selected. Although it is extremely implausible, an assault may utilize 51% of the system's processing power. As a result, blockchain is among the most dependable and secure solutions

CC BY NC

available today. As others have noted, blockchain technology is very expensive to use. All fees are the responsibility of the individual who requests the estimate. The value of Ethereum Classic (ETH), which is required for gas fees on the Ethereum network, is approximately $120 USD as of January 2019, according to EthereumPrice.org. Institutions couldn't afford to manage the required volume of transactions. Databases, illness registries, electronic health records (EHRs), and personal health records would all be replaced by a blockchain system. This demonstrates the obvious outcome that follows.

Applying a global ledger technique. The individual who requests the estimate is responsible for paying any fees. The value of Ethereum Classic (ETH), which is required for gas fees on the Ethereum network, is approximately $120 USD as of January 2019, according to EthereumPrice.org. Institutions couldn't afford to process that many transactions. A blockchain-based healthcare system would replace patient medical records, electronic health records, disease files, and other databases. Eliminating needless errors and data breaches would increase the system's cost-effectiveness.

6. CONCLUSION

Because blockchain technology is safer and more effective, it is a good idea to employ it in several areas of the healthcare system. This approach may be helpful for storing and transmitting medical and insurance records to and from locations such as clinical trial sites, hospitals, mobile devices, and remote monitoring systems. Although there aren't many studies on blockchain's potential applications in healthcare, they are gradually increasing. Currently, one of the most researched areas in computer science is blockchain. The healthcare system may be significantly impacted if patients have greater control over their medical data and information. Although blockchain technology is still in its infancy, it has the potential to improve individualized healthcare.

REFERENCES

1. Journal H (2018) Largest Healthcare Data Breaches of 2018. HIPAA Journal.
2. Nakomo to (2008) Bitcoin: A Peer-to-Peer Electronic Cash System.
3. Antonopoulos AM (2014) Mastering Bit coin: Unlocking Digital Crypto currencies. O'Reilly Media, 2014.
4. Ichikawa D, Kashiyama M and Ueno T (2017) Tamper-Resistant Mobile Health Using Block chain Technology. JMIRM health U health 5(7): e111.
5. Yue X, Wang H, Jin D, Mingqiang Li, Wei Jiang (2016) Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst 40: 218.
6. GriggsKN, OssipovaO, Kohlios CP, Alessandro NBaccarini, Emily A Howson, et al. (2018) Healthcare Blockchain System Using SmartContracts for Secure Automated Remote Patient Monitoring. J Med Syst42:130.
7. Firdaus A, AnuarNB, RazakMFA, IbrahimAbakerTargio Hashem,Syafiq Bachok, et al. (2018) Root Exploit Detection and FeaturesOptimization: Mobile Device and Blockchain Based Medical Data Management. J Med Syst 42: 112.
8. Fan K,Wang S,Ren Y,LiH, YangY (2018)Med Block: Efficient and SecureMedicalDataSharingViaBlockchain.JMedSyst42: 136.

CC BY NC

9. Li H, Zhu L, Shen M, Feng Gao, Xiaoling Tao, et al. (2018) Blockchain-Based Data Preservation System for Medical Data. J Med Syst 42: 141.
10. Roehrs A, da Costa CA and da Rosa Right R (2017) OmniPHR: A distributed architecture model to integrate personal health records. JBiomed Inform 71: 70-81.