wjert, 2019, Vol. 5, Issue 6, 290-299. *Review Article* **ISSN 2454-695X**

World Journal of Engineering Research and Technology
WJERT
www.wjert.org

SJIF Impact Factor: 5.924

BLOCKCHAIN IN HEALTHCARE: A REVIEW

***Apoorva Chouhan and Dr. Praveen Srinath**

MTech CS, MPSTME, NMIMS University, Mumbai.

Article Received on 13/09/2019 Article Revised on 23/10/2019 Article Accepted on 03/11/2019

***Corresponding Author**
Apoorva Chouhan
MTech CS, MPSTME,
NMIMS University,
Mumbai.

ABSTRACT

Blockchain provides the promise of trust and security. In the healthcare space, it is speculated to enable patient centric care, secure data storage with enhanced privacy, transparent information exchange and improve quality of services and health worldwide. Blockchain brings with it a disruption of the traditional systems that poses unique domain challenges. As the technology matures and is widely understood, it finds solutions to some of the major healthcare challenges globally. This paper reviews the principles of blockchain, challenges in healthcare and how blockchain addresses a few of them, potential use cases for the domain, obstacles in the adoption of the technology and a some implementations with focus on compliance with General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA).

KEYWORDS: *Blockchain, healthcare, GDPR, HIPAA.*

I. INTRODUCTION

Healthcare industry awaits the next innovation curve. Technical advances have improved health systems over the years, with increased reach and accessibility. However, the industry has been paced down by stringent regulations and standards that limit the acceptance of technology. Technology has revolutionized innovation and research in the health space, artificial intelligence and machine learning have facilitated for faster and more accurate patient monitoring, symptom detection, diagnoses and preventive care. As most sciences now depend on the massive volume of data generated to innovate, so does Life sciences. Health data is an increasingly abundant resource that can be harnessed to create opportunities where challenges currently exist in the industry. Experts from both Health and Information Technology eagerly look forward to Blockchain as the step ahead.

II. BLOCKCHAIN PRINCIPLES

Distributed Ledger Technology includes blockchain technologies and smart contracts. While distributed ledgers existed prior to Bitcoin, the Bitcoin blockchain marks the convergence of a host of technologies, including timestamping of transactions, Peer-to-Peer (P2P) networks, cryptography, and shared computational power, along with a new consensus algorithm. Blockchain is a specific form or subset of distributed ledger technologies, which constructs a chronological chain of blocks, hence the name 'block-chain'. A block refers to a set of transactions that are bundled together and added to the chain at the same time. In the Bitcoin blockchain, the miner nodes bundle unconfirmed and valid transactions into a block. Each block contains a given number of transactions. Consensus algorithms are used to determine the miner node for the next block on the chain. Blocks of transaction are iteratively hashed to strengthen security and immutability.

Smart contracts are simply computer programs that execute predefined actions when certain conditions within the system are met. Consensus refers to a system of ensuring that parties agree to a certain state of the system as the true state. Mining is the process of validating transactions in a proposed block and appending it to the chain if successfully validated, performed by nodes on the network.

III. EXISTING CHALLENGES IN PERSONAL HEALTH MANAGEMENT

As Healthcare Technology moves on to the next innovation curve globally, a large section still struggles with providing quality care to individuals, and at times even basic care. This is largely due to the fragmentation within the healthcare space. User data is owned by and stored with different participants, there is limited support for large scale remote monitoring and care, Manual handling of patient data often leads to illegal practices and violation of user privacy. These factors negatively impact the quality of care received, interoperability, availability of health systems thus eventually degrading user well-being. Most of these limitations can be traced down to the following technological challenges:

1) Lack of digitization is one of the major challenges. Healthcare across the globe is going through a shift from physical paper records to Electronic Health Records (EHRs). Maintaining patient data manually on paper and storing such data at a large scale greatly reduces its security and availability. It is prone to human errors and can often be lost or

illegally used. Digitization of such sensitive data is the next big step for National Healthcare policy makers.

2) This decade has seen a shift in the Healthcare industry from physical patient records to Electronic Health Records (EHRs). This movement to digitize data came with its own opportunities and challenges, some being: a. Maturing EHR models and vast growth in medical data by volume and type, increases the need for secure data storage and access. b. Focusing on interoperability of patient data for a seamless Healthcare experience. Agreeing on global guidelines and standards to achieve such interoperability is a continued effort. c. Educating all stakeholders in the usage of EHRs.

3) Integrating Remote data sensing and healthcare. With the onset of IoT (internet of Things) wearables have increasingly become a part of user lifestyle and thus play a vital role in live data reading and remote care. IoT devices, connected to cloud or fog are extremely vulnerable to cyberattacks. Therefore, interoperability and data security are major challenges.

4) Healthcare is highly centralized and operated privately. The ownership of patient data has always rested with the providers. Making healthcare patient centric, decentralizing ownership of information is the need of the hour.

4) Information overload and Clinician burnout with EHRs. Medical staff can be faced with overwhelming amounts of data that needs to be understood and used in the right context.

5) Medical Research faces the challenge of a fragmented industry. Sensitive patient data changes multiple hands moving in between institutions and researchers. Data breaches, illegal use and monetization of personal data are common malpractices.

6) Healthcare data breaches are frequent and highly damaging. These may occur because the data transactions are not verifiable and can be tampered with, exposing user data to be used without consent, which is a violation of the GDPR regulations.

7) 3.5 Million patient records were compromised in data breaches by Q2 of 2018. With growing adoption of cloud and mobility solution in the healthcare sector, data today has more value than any other commodity, making hospitals, patient health records, doctors' offices, pharmacies the prime targets due to abundance of health data.

8) Patient Consent in data sharing is the primary concern worldwide in the Healthcare space. With strong regulations in place that aim to enforce privacy and transparency in use of personal data by healthcare providers, managing patient consent is on the immediate focus. Efforts are being made to increasingly hand over control of personal data to the patient and practice request-grant based access control to sensitive information.

9) Securing the data that is already available online is also an area that needs standards and guidelines such as encryption policies, security for data in virtual machines and on the cloud, access controls to sensitive data. HIPAA and GDPR are guiding frameworks to follow and strengthen security in Personal health data management.

IV. OPPORTUNITIES FOR BLOCKCHAIN IN HEALTHCARE

1) Blockchain enables Decentralized Trust via mathematical models and encryption algorithms within transacting participants that need not know each other. This provides a vast scope for Personal Health data sharing between patients and healthcare providers. This ensures that only verified participants are allowed to transact with each other.

2) Blockchain provides an 'Append-only' ledger, meaning that new transactions are added on to the chain without modifications to the existing ones, making it Immutable. Sensitive personal Health data added to the chain remains Tamperproof unlike physical records that are easily compromised.

3) A single truth of events is maintained by consensus amongst all participating nodes in a blockchain network, making it the most Reliable source of information in times of conflict. This solves the problem of sharing of data without user consent or outside their knowledge. Only access requests accepted by the patient to specific data sources are verified as transactions on the chain.

5) Patient Data undergoes many levels of encryption, maintaining high levels of Privacy, which has been a growing concern globally.

6) All participants are nodes in the decentralized network and have equal rights and access to the ledger, enabling Transparency and verifiability of all events that are recorded on to the chain. Therefore, in the healthcare space, patients and providers have equal rights as nodes on the network for fair interactions. Therefore, control rests with the consensus and not owned by a single entity.

IV. USE CASES

Healthcare policy makers and blockchain experts are collaborating to come up with impactful blockchain solutions that promise to solve challenges in the health space. A few of the use cases for blockchain in healthcare are mentioned below.

1) Medical Registry- Provider Identity management Information stores of Healthcare Providers are coming into light fairly recently. Secure databases to store provider details, qualification, certifications and history of practice with an added layer of security and immutability via blockchain are an interesting application to improve fluidity of provider information and quality of service delivered to the patients.

2) Patient Registry – Identity management

Blockchain allows a structured approach to control patient data in from disparate provider sources. Consolidation of such data with better ease leads to improved use of and access to critical information by providers, specialists, researchers and for clinical trials.

3) Secure Electronic Health Records

Patient data storage has seen a shift from physical records to Electronic Health Records (EHRs).Migrating massive volumes of on-paper patient data to cloud or silo databases is not without its challenges and limitations. Healthcare data breaches are a reason for concern across the globe, as it compromises highly sensitive patient information.

Blockchain powered EHRs increase security with the use of encryption and access controls over on-chain and off-chain data. It also leverages the benefit of tamper proofing to curb any attempts at manipulating user information.

4) Patient centric Data sharing

Ownership of Patient data has historically rested with the Healthcare providers. Blockchain can be leveraged to build a data sharing ecosystem that is patient centric i.e. allows patients to control the mobility of their information. Providers such as Physicians, Specialists, Clinical Researchers, etc. request to access patient data and patient can grant access or decline the request based in their consent. This facilitates increased privacy and transparency over shared information.

5) Prescription Provenance

Seamless data exchange can be enables between Doctors and Pharmacies to track legitimacy of prescriptions. Prescriptions stored as transactions on the chain can be used for auditing drug usage and sales, disregarding any fraudulent prescriptions.

6) Pharmaceuticals and Drug Supply chain

Blockchain has found a soft spot in provenance for supply chain management. In the healthcare industry, one major supply chain that raises reasons for concerns is the Pharmaceuticals and drug manufacturing chain. These processes often get manipulated to produce and sell drugs with illegal contents, which can cause harmful effects on consumption. Blockchain solutions in the space will enable auditing and tracking of the supply chain process with all manufacturers, chemists, sellers operating in transparency.

7) Organ Donation Platform

The gap between number of patients in need of a transplant and willing registered donors is a major challenge in healthcare. Lack of trust between potential donors and those involved in the process of transplantation is often cited as a reason for this gap amongst others. Blockchain enables organ donation and transplantation platform can increase security and traceability of in the system, preventing manipulations that limit the impact of donations on the rightful patients.

VI. LIMITATIONS

1) Acceptance and Incentives

Acceptance of and adherence to new technology is challenge, even more so with blockchain as it brings about a fundamental disruption. This decade has already seen a massive migration of information from physical systems to cloud data storage in healthcare. The challenge at hand is to cultivate an awareness and a willingness amongst all players towards blockchain. This requires an insightful understanding of the pain points in the healthcare space and if blockchain can provide a solution, thus incentivizing the acceptance towards this new disruptor.

2) Regulatory challenges

As Healthcare is a safety critical industry, it follows stringent regulations and policy makers should consider them in the context of Blockchain. Ownership and governance of information on the chain requires elaborate discussions between all involved providers. It is also bound to follow the GDPR and HIPPA regulations, some of which are as follows.

- Organizations must be responsible for using subject’s data for legitimate purpose only and inform the subjects about the processing activities on their personal data.
- When an organization have intent to process personal data for a legitimate purpose or beyond, for which that data is collected, a clear and explicit consent must be taken from the data subject.
- The subject has the right to ask organization what information about them it holds, they have right to make correction, anonymize data, and delete or transfer their personal data.
- Article 17 focuses on the ‘Right to be forgotten’, meaning that users may, at any time, request to have all their data removed or ‘erased’ from the systems.

- The Organization is responsible for providing security during collecting, transferring and processing personal data. In case of data breach, appropriate notifications must be given to the regulator and subject within 72 hours.

- **HIPAA Privacy Rule**

The patient has right to examine, make corrections and retain the health records in the form and manner they request. It permits the use and disclosure of health records needed for a meaningful purpose. It applies to covered entities.

- **HIPAA Security Rule**

Secure maintenance, transmission and handling of ePHI ensuring confidentiality, integrity and availability. There must be physical, administrative and technical safeguards in Healthcare Organization. This rule applies to covered entities and business associates.

- **HIPAA Breach Notification Rule**

On Occurrence of breach, Minor or Meaningful breaches depending upon scope and size along with appropriate protocol changes should be reported to HHS OCR (Health and Human Services Office of Civil Rights), applying to both covered entities and business associates.

3) Implementation and integration

Healthcare is a highly fragmented industry and most of the data is stored in silos by individual providers. Creating an ecosystem for interoperability would first require a lossless integration of these varied data sources, for seamless exchange.

VII. MAKING BLOCKCHAIN HIPAA-GDPR COMPLIANT

1) Encryption. HIPAA does not prescribe specific methods or tools for how to secure data; however, encryption is encouraged as a best practice. It is general practice to encrypt every transaction record with a public-private key pair, storing the encrypted information on the chain. When there is a request to remove user data, the key pair is discarded, rendering the on-chain encrypted data unusable.

2) Store Personal data off-chain, Hash digests on-chain. Reference Links along with hash and metadata are to be stored on the blockchain. In cases where deletion of data is requested, it can be removed from the off-chain database and only the hash of it remains on the blockchain. Since hashing is one way, there is no way to discern the original information from the chain.

CRUD vs CRAB

Traditional databases follow CRUD operations – Create-Read-Update-Delete. Whereas, Operations on blockchain can be described as: Create-Retrieve-Append-Burn . Append replaces Update, as any modifications to pre-existing data are implemented only as new transactions on the blockchain. Burn refers to throwing away links/keys to disallow new transactions to be appended to the world state of an asset. This can be carried out by forgetting the private key or setting it to an 'unsolvable' key by choosing a random public key thereby locking everyone out of the asset. More commonly, it is done by throwing away encryption keys so it cannot be decrypted.

3) Private Data. It is a newer concept that uses policy logic already present in Hyperledger Fabric with AND, OR operators to add to the existing access rights. This allows to create collections of data using policies to define which parties in the channel can access the data , access can simply be managed by adding policies to the collections. Allows for some data to be public and some to be private. Limitations of usage:

a) Data is kept only as long as it is being used. A 'blockToLive' parameter can be specified with the policies that defines how long a collection should be kept within the blocks, after which it is automatically purged.

b) Does not allow access to data that is not being used.

c) Right to be forgotten is practiced as items can be removed from the policies leaving only the 'unusable' hash on-chain.

4) To allow interoperability of Electronic Health Information, while keeping everything completely protected, Blockchain within **HIPAA compliant Cloud Database** is a solution. Some HIPAA compliant cloud databases are:

Dropbox: Administrative controls include review and removal of linked devices, user access, user activity reports, and enabling two-step authentication.

Google Drive: Covered applications include Docs, Sheets, Slides, and Forms as well as several other services such as Gmail. Administrative controls include account activity and app activity tracking, audits, and file-sharing permissions.

Microsoft OneDrive: Offers some of the best security practices in the industry and supports HIPAA.

5) SimplyVital in the Health Nexus platform introduces a blockchain framework that provides secure HIPAA compliant protocols for the first time. Tracking activity in healthcare technology platforms is a requirement of HIPAA and is carried out using Health Tokens. Access to data is given using keys by a governing consortium that acts as a whitelist that exists to focus on healthcare security compliance. Built in key-pair system allows user to grant access to healthcare data by creating permissioned keys. The data can be stored off the blockchain, but the key pair system allows you to grant access to this "off chain data." A master key allows creating, tracking and managing children keys. A governance and validation protocol ensures to make every miner on the node HIPAA compliant. This layer also creates a governing consortium that votes and approves upgrades, creating a smoother and faster system for updating the network.

6) MedRec proposes a solution by requiring all miners to be fully permissioned and medical researchers running mining nodes only to do so on secured systems. MedRec encourages the addition of encryption in the off- blockchain synchronization steps, safeguarding against accidental or malicious content access. Another proposed solution to the problem of privacy is to use a system of 'delegated contracts', where each provider creates a separate Ethereum identity for each new Patient Provider Relationship. In order for the relationship to be created securely, however, the provider could not append the fresh block containing this new address itself (as it would be simple to trace back each of these delegate addresses to the original). Thus, on creating a new delegate account, the provider performs an off-blockchain transaction with verified providers at random, giving them the details of the new delegate account, which they may append as a verified account to the blockchain.

7) User centric data sharing. Proposed systems rely on users to manage consent and access requests over their personal information. Data storing strategy is such that all static or gradual dynamic, lightweight data goes on to the chain itself and use of cloud databases to store encrypted, continuous, dynamic data (off-chain) .Transactions like upload, request and response are recorded on the blockchain in a format comprising of the asset public key, action and encrypted link to the data. Users review and respond to incoming requests for access permissions over their information, ensuring consent in data sharing. Entities known as key-keepers manage the transfer and allocation of private keys over access granted assets.

VIII. CONCLUSION

Blockchain creates interesting opportunities in healthcare with secure information exchange, provenance in drug manufacturing adn supply, service provision, remote care, integration with IoT amongst others. It looks to seamlessly integrate the fragmented industry into an ecosystem of health to improve the quality of life for all. In doing so, it faces unique challenges in implementation and acceptance. Global standards and regulations for blockchain in healthcare can accelerate the disruption and allow to leverage the technology to solve some of the immediate health concerns globally.

IX. REFERENCES

1. Andrew Lippman, Ariel Ekblaw, Asaph Azaria, John D. Halamka," A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data", MIT Media Lab, August 2016J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
2. RJ Krawiec, Dan Housman, et. al.,"Blockchain: Opportunities for Healthcare", August 2016K.
3. Lucas Hendren and Katherine Kuzmeskas, "Health Nexus", 2017 SimplyVital Health, Inc.
4. N. Satoshi (2008), Bitcoin: A Peer-to-Peer Electronic Cash System, [Online]. Available: https://bitcoin.org/bitcoin.pdf
5. G. Prisco (2016, April), The Blockchain for Healthcare: Gem Launches Gem Health Network With Philips Blockchain Lab, [Online]. Available: https://bitcoinmagazine.com/articles/the-blockchain-for-heathcare-gemlaunches-gem-health-network-with-philips-blockchain-lab-1461674938
6. https://www.hipaajournal.com/
7. https://eugdpr.org/
8. Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom). doi:10.1109/healthcom.2016.7749510