Journal of Engineering Sciences

Vol 11, Issue 6,June/2020
ISSN NO:0377-9254

Blockchain: An assured technology for protecting Healthcare in post COVID-19 era

Aanchal Yadav (M.Tech in Data Science), Supervised By: Dr. Jawed Ahmed
Author[1] Jamia Hamdard, New Delhi, India
Author[2] Jamia Hamdard, New Delhi, India
yadavaanchal96@gmail.com , jawed2047@gmail.com

Abstract

There have been disputes in healthcare from the complex network of mediators and the lack of traceability of transaction and security of data. To mention post COVID-19 era only some healthcare statistics is disjointed across several depository unconstructively distressing research and services, about 50% of the clinical trials are never reported, the expenditure of drug discovery and patients recovery is constantly increasing, and third-rate and fake medicines are still a big problem in healthcare industry. Blockchain has the potential to resolve these problems as it provides trust without any intermediaries, has traceability as a default characteristic, and promises new business models by permissive novel incentive structures. Due to its potential, blockchain has gathered Compelling interest in the healthcare industry. In this paper, authors reviews key usage of blockchain in healthcare mentioning post COVID-19 era: patient data management, supply chain management of medical goods, billing claims management, and analytics. Authors established that most of the blockchain projects are partial as white-papers, proof of concepts, and products with a limited user base. However, it was observed that the quality, quantity, and development of the projects are rising.

We also discuss technical and business challenges to the implementation of blockchain in the healthcare industry.

Keywords: Blockchain, Health care, COVID-19, Traceability, Data management, Supply chain, analytics.

1. Introduction

Authors try to review the literature on implementation of the Blockchain and similar digital ledger techniques in various other domains of health care and specially data security beyond its application to crypto-currency and to draw appropriate conclusions assuming post COVID-19 era. Blockchain being somewhat a new technology, a represent able sample research is obtainable, crossing over the last ten years, initially from the early on work in this field. Differential procedure of Blockchain and other digital ledger techniques, their challenges, applications, security and privacy issues were examined. Identifying the most hopeful path for potential use of Blockchain beyond crypto-currency is the major focal point of the review study. Blockchain (BC), the technology supporting Bitcoin crypto-currency system, is measured to be vital for assembling the backbone for ensuring improved security and privacy for various applications in many other domains including the Internet of Things (IoT) eco-system which can now also play a vital role in Health care domain in respect to its data availability and security. International research work is being carried out in both academic and industrial domains applying Blockchain in varied forms.

The Proof-of-Work (PoW) mathematical challenge establishes Blockchain security by maintaining a digital ledger of transactions that is considered to be unchangeable. Furthermore, BC uses a changeable Public Key (PK) to proof the users' uniqueness that provides an extra layer of privacy. The successful implementation of Blockchain has been put into action in diverse non-monetary systems such as in healthcare data security distributed cloud storage systems, decentralized messaging, proof-of-location, and so on.

Recent research articles and projects were scrutinized to establish the implementation of Block Chain for improved security and to identify its associated challenges and thence to propose solutions for Blockchain enabled enhanced security systems. The understanding domain of the research is in the area of the healthcare, specifically, in Blockchain.

1.1 Essentials of Blockchain

A Blockchain constitute of two different components, as follows:

1. **Transaction:**

A transaction, in a Blockchain, symbolizes the act triggered by the participant.

2. **Block:**

A block, in a Blockchain, is a group of data logs that the transaction and other associated details such as the correct sequence, timestamp of creation, etc.

Blockchain can either be public or private, depending on the extent of its utilization. A public Blockchain authorizes all the users with read and write permissions such as in Bitcoin. On the other hand, there are some public Block chains that edge the access to only either to read or to write. While on the converse, a private Blockchain restricts the admission to select trusted members only, with the aim to keep the users' details hidden. This is particularly applicable amongst governmental institutions and associated ally or their aid thereof. The foremost perks of the Blockchain are that its execution technology is public. Each participating article possesses an entire updated record of the transactions and the allied blocks. Thus the data remains unaffected, as any change would be publicly confirmable.

However, the information in the blocks is encrypted by a private key and hence cannot be translated by everyone.

Additional advantage of the Blockchain technology is its decentralization.

It is decentralized in the sense that:

• There's no single device that stores the data (transactions and associated blocks), rather it's distributed amongst the members throughout the network supporting the Blockchain.

• The transactions are not subject matter of approval to any single authority or have to follow set of specific rules, thus involving considerable trust as to reach consent.

• The overall security of a Blockchain eco-system is an additional advantage. The system only allows new blocks to be adjoined. Since the previous blocks are public and distributed, they cannot be altered or amended.

For new transaction to be part of the existing chain, it has to be ascertained by all the participants of the applicable Blockchain eco-system. For such a rationale and verified process, the participants must apply a precise algorithm. The applicable Blockchain eco-system defines what is apparent as "valid", which may differ from one eco-system to another. A number of transactions, thus approved by the rationale and verification process, are grouped together in a block. The newly ready block is then corresponded to all other participating nodes to be appending the existing chain of blocks. Each later block contains a hash, a unique digital fingerprint, of the previous one. Figure 1 determines how Blockchain transactions take place, using a gradual example. Bob is going to transport some money to Alice. Once the financial transaction is initiated and hence prompted by Bob, it is represented as a "transaction" and broadcast to all the concerned parties in the networks. The transaction now has to get "authorization" of being indeed "valid" by the Blockchain eco-system. Transaction(s) once accepted as valid along with the hash of the later block are then fed into a new "block" and communicated to all the participating nodes to be subsequently adjoined to the existing chain of blocks in the Blockchain digital ledger.

Figure 1. Operation of the Blockchain.

Source:https://www.investopedia.com/terms/b/blockchain.asp

2. Why Blockchain for DataSecurity?

Trust and traceability are the two basic commitments of the blockchain accessed out of the box which determine the general trust problem on the community, and organization. However, these characters are not always satisfactory to provide a complete solution, which is why we often see blockchain opposite with strong cryptographic protocols like zero-knowledge proofs. This pairing establishes to provide traceability, security, trust, and be in command of which are the core building blocks for serious solutions in several industries including health care and supply chain. Data documented in the blockchain cannot be altered or destroy without leaving a mark out. This dependability and traceability of the data is a serious requirement for any health care system. Thus, the resources of blockchain seem impending.

Here, we list some of the core concerns that need to be addressed in health care solutions:

•Secure storage and integrity protection
•Privacy and ownership of data
•Data sharing
•Traceability and accountability of data

While each of these involvements can be addressed independently with the proper use of cryptography and privacy-preserving technologies, the major concerns in such solutions have always been the prevailing trust model. In such solutions, blockchain as a confiding decentralized ledger technology can take action as a trust necessary glue. Despite the immense potential, there are restrictions as of the current state of the blockchain. Currently, every node in the network practices the transaction which makes the blockchain rather time-consuming and inappropriate to handle real-world transactions which vary in tens thousands of transactions per second. This inequality highlights the scaling concern that block chain have to conquer for deep implementation across all industries. Furthermore, with the increase in usage, the size of blockchain is increasing enormously, making it complicated for normal users to keep the full replica of it. On an optimistic note, with vast investment and research efforts invested into blockchain, a better scalable version may develop in the future. Decentralization, consistency, and scalability (DCS) are the three pleasing properties that blockchain platforms struggle to maintain. Blockchain technology can only concurrently provide two out of three properties; there will always be a trade-off. Softwares like Bitcoin and Ethereum are DC system where they make available sufficient decentralization and consistency of data but lack scalability. On the other hand, Hyper ledger is an example of a CS system which ensures data consistency and can scale above 10K+ transactions per second at the cost of losing decentralization. In the last decade, it was observed the growth of blockchain in three generations. Crypto currencies defined the first 1.0 generation which was mainly designed as a substitute payment system. Then, decentralized applications based on smart contracts represented the 2.0 applications provided that business logic concept and execution on a trusted platform where safety and security of smart contracts is the key issue. Smart contracts which can be justified and tested before exploitation on a live blockchain prevent financial losses due to flaws in the code. The third generation is taking a persistent multi-dimensional approach connecting Internet of Things (IoT), machine learning, and different branches of science. These different generations of blockchain are growing simultaneously in their own velocity, inscribing the issues like privacy, scalability, and security and along the way.

3. Healthcare Data Management

The Health Care Data Management which comprises storage space, access control, and sharing of the data is a significant aspect of the healthcare industry. Appropriate management of healthcare data advances healthcare outcomes by allowing comprehensive views of patients, personalized treatments, and efficient communication. It is also serious for working healthcare industry cost-effectively and efficiently. However, running healthcare data is a demanding task due to its sensitive nature and successive trust issues. And it is one of the main reasons why the healthcare system is disjointed with healthcare information and services exist in dissimilar forms in several silos. This disconnected system is a reason for several inefficiencies' in healthcare and is a key obstacle for healthcare research. Healthcare professionals generally do not have right to use to the complete information of patients, thereby, obstructing the subsequent diagnosis and treatment steps; and researchers put effort to find the preferred data for

their studies, thereby, reducing down healthcare research. Blockchain may facilitate the efficient sharing of healthcare data while establishing data reliability and protecting patient privacy. Safe, efficient, cost-effective, and accountable can be built with its precise use alongside with other technologies. In addition, the implementation of blockchain can compel forward the movement of patient-centric healthcare model where patients control their healthcare data. The key difficulties behind data-sharing in both patient-centric and traditional models are because of lack of trust and lack of incentives to contribute to. The blockchain technology can explain both tribulations by performing as a trust layer and introducing the incentive mechanisms such as rewarding crypto tokens for sharing data. Moreover, blockchain can be the link for the integration of medical data and healthcare records and internet of things; the healthcare and lifestyle data composed by devices can be critical for correct diagnosis but are underutilized since there is a lack of a way for a physician to access the patient-generated data. With blockchain-enabled trust and motivation configuration, there is a promise for a global HIE and a marketplace on top of it. But the lack of regular healthcare data standards can be one of the major obstacles to overcome before the development of an interoperable HIE connecting multiple disparate data silos. However, there is a possibility that the incentives introduced by blockchain-based data replace may fuel the establishment and the development of the open data standards.

Blockchain technology would be an exciting use case that requires the balance among efficiency, privacy, and transparency. Moreover, country-specificity regulations will be another obstacle for a HIE connecting multiple regulatory regions.

3.1 Blockchain Technology for health care data management

Many companies are focusing on emerging some form of blockchain and providing data and services marketplace overhead of it. Among them, some are focusing general electronic health records (EHR) data while some are specializing in particular data methods such as genomics and dermatology. For example, Medrec is an open source blockchain platform for EHR management. It was lately tested in collaboration with Beth Israel Deaconess Center. Patientory is one of the early blockchain based healthcare venture introduced to leverage Initial Coin Offerings (ICO) for funding.

Testing is carried out by Health Suite Insights of Philips Healthcare verified Data Exchange Process, a product that allows the secure and traceable data exchange between the members within a system of hospitals and medical universities; all the data interactions is within the network are stored in a blockchain together with the identities of the people performing the exchanges to create an audit trail of the data exchange. Medshare provides a blockchain based data sharing of electronic medical records among entrusted parties by introducing data origin, auditing, and trailing on medical data. Utilizing smart contracts and an access control system, they claim that their system can successfully trace the behavior of the data and withdraw access to violated rules and permissions on the data. Iryo is creating a global depository of health data in OpenEHR format.

Figure 2: Healthcare Suits and Companies

Source: google.com

4. Cybercriminals exploiting fear game of rising COVID-19?

After the inconsistent increase of COVID-19 cases in 2020 India and globally comes the never-ending techniques cybercriminal use to attack on public panic amidst the global pandemic, and the critical information/data in today's scenario which is vital for the forthcoming of Nations post COVID-19.
Kaspersky total security Antivirus, also revealed emails offering products such as masks, and then the issue became more frequently used in Nigerian spam emails. Researchers also established scam emails

with phishing links and malicious attachments.

These kinds of activities could adversely affect the data and its security in Healthcare.

One of the latest spam campaigns resembles the World Health Organization (WHO), showing how cybercriminals are recognized and are capitalizing on the significant role WHO has in providing trustworthy records and data about the COVID-19 cases. This is mentioned by David Emm, Principal Security Researcher that "We would encourage companies to be particularly vigilant at this time, and ensure employees who are working at home exercise caution. Businesses and Industries should converse clearly with workers to ensure they are aware of the risks, and do everything they can to secure remote access for those self-isolating or working from home,"

Some malicious files are spread via email. For example, an Excel file circulated via email under the appearance of a list of COVID-19 patients supposedly sent from the World Health Organization (WHO) was, in fact, a Trojan-Downloader, which surreptitiously downloads and installs another malicious file. This subsequent file was a Trojan-Spy designed to group various data, including passwords, from the infected device and provide it to the attacker.

5. Billing Claims Management shifts towards Cloud post COVID-19

Financial aspects of medical care are essentially important in the healthcare landscape. This area of financing phase in healthcare is common with inefficiencies', mostly related to the belief and transparency, which can potentially be optimized by the use of blockchain. Blockchain provides a system for direct associations between patients (one who makes claims) with the carrier (one who clears the claim), as there is conviction inbuilt. Smart contracts could be used in the premium negotiating aspects. Data relating the current health status of the victims, medication usage, etc. attached through blockchain to developing premiums, through smart contracts. When many parties are implicated in the claim handling, there might be a lot of recurring tasks and checks involved which might be oppressive for the end customer. After seeing these contingencies for improvements, some hypothesis has been brought into view using blockchain for billing claims management and broader financial aspect of care delivery in post COVID-19 era. Gem is using Ethereum to streamline the claim management in healthcare services, among others. It brings the patients, providers, and the insurers together into one network to provide real-time observations into patient's health journey and simplicity health claims management. Change healthcare is using the Hyper Ledger Fabric framework for blockchain related claims and revenue management. Several healthcare companies, including insurers like Humana and United Healthcare, have been operational on a pilot program using blockchain to continue and distribute curetted information from healthcare providers. This characteristic can resolve a lot of redundancies and inefficiencies' related to insurance claims management.

6. Challenges

Although blockchain dominates great potential to advance and signify to the healthcare system and several companies have already started testing it for specificity use cases, there are several challenges to be accepted before its mainstream practice. There are various aspects to the challenges on the mainstream adoption of the blockchain technology. These aspects are for example: • Technical • Legal • Business • Trust issues

In this section, author touches upon some of the challenges to be predictable for the wide practice of the blockchain technology in the healthcare sector.

6.1 Interoperability & integration with the legacy systems

Healthcare space has a huge number of technologies, devices, and components, not obliterating the personnel, which all come mutually to solve the current needs in the space. There are large rooms for advancement, with blockchain technology providing a guarantee to cover up some of this room. However, the blockchain technology would still be just one piece, though likely very vital, of the puzzle. The blockchain technology has to incorporate well with

existing systems, and the incorporation is going to be a demanding tribulation because of several reasons such as interoperability. That's why the healthcare space has multiple numbers of devices and their types make it even more complex.

All applicable parties and stakeholders should all come simultaneously to make the use of blockchain technology more persistent in healthcare. If blockchain cannot be a catalyst for this cooperation between stakeholders and relevant parties, then it probably does not have much worth above and further than being a simple and functional tool to solve some issues around trust. Many of the other concerns around ecosystem building would still be present, regardless of the blockchain.

A significant feature of this research also describes to the preparation of healthcare IT personnel. These personnel might be needed to be re-trained on blockchain technology if the blockchain technology would enter into the healthcare space, it would definitely help in protecting data security and transactions.

7. COVID-19 outbreak raises Frauds?

With outbreak of COVID-19 globally the purchase and all tractions along with the data turns towards digitalization which also mentions the requirement of Cloud Computing for data store and security. The COVID-19 pandemic has given rise to a new harmful threat: fraudsters, who victimize on vulnerable individuals/organizations and seek to make use of this terrible humanitarian calamity for their own benefit. Organizations' should therefore need to be more alert and build robust mechanisms to discourage fraud in these difficult times and specially post COVID-19 recovery time.

Among the range of sectors, consumer markets have been intensely jolt as strict lockdowns have brought economic to a standstill. Weakening demand for non-essential products and interruption in raw material supplies has squeezed the profitability and cash flows of several organizations in the sector. Demand could also take a hit on cutting down salary and job losses tighten the purchasing power of consumers in the wake of the COVID-19 outbreak. Even as the consumer markets sector has been facing major set challenges, it has triggered more opportunities for organized criminals to defraud consumers and organizations by violating security.

Organizations' and consumers need to be on their own guard in various kinds of fraud and other wrong activities that could come forward as a result of the pandemic.

- **Sales and distribution**: the exploitation of schemes, unnecessary price inflation due to lack of essential products, and the sale of damaged or expired products because of apparent shortages of essential products during the lockdown.
- **Fake online websites/social media accounts:** these might attract consumers to pay blunt for the products. After receiving the payment, fraud people pocket this money without delivering the products.
- **Cyber crimes due to increased remote working and amplified digital transactions:** due to the lockdown of brick-and-mortar outlets, and healthcare transactions etc.
- **Reduced focus on fulfillment that triggers breaking of laws and regulation:** on the increased operational challenges and remote working.

Increase in cases of COVID-19-related fraud, could bang the overall governance and transparency, even distort markets and shake the faith of the investment community.

8. Conclusion and Scope

Blockchain technology has the prospective to answer several problems disturbing the healthcare industry today. As a trust mediator, it can facilitate novel healthcare solutions; and as an inducement machine, it can allow novel business models that may guide to a new dynamics among a range of healthcare stakeholders like patients and providers. For example, a patient-centric healthcare model and a global HIE might be executed by virtue of blockchain allow decentralized trust and incentive structures. Similarly, blockchain based decentralized network/services may reduce vendor lock-in problems in healthcare.

In this paper, authors reviewed major uses of blockchain such as healthcare data management, supply chain management in the pharmaceutical industry, billing/claims management, analytics, etc. Examples of organizations emerging blockchain-based applications for these use cases were also accessible. The proposed application trying to build a complete decentralized health care ecosystem to specificity applications such as data origin, counter fit drugs identification, consent management, etc. Regardless of the vast potential of blockchain technology and an enormous amount of interest around it, we found that its impact on healthcare is minimal and is still in the early days. Most of the blockchain based healthcare explanations are still in the form of novel concepts represented by whitepapers, prototypes, or only a very small number of working products with a limited user base. However, the field is growing rapidly; we expect an efficient positive impression of blockchain in healthcare in the future. Challenges such as interoperability, integration with the existing systems, uncertainty in cost, technological and adoption barrier, regulatory compliance, and scaling needs to be successfully tackled to help blockchain make its mark in the healthcare industry.

It may be found that, if a blockchain is stored on each network node, then services or authorities cannot shut down a blockchain. If blockchain is not centralized or controlled by a point, then there is no chance to close a blockchain.

Arguably this is a delusion.

The challenge here is avoiding concentration. A blockchain is only as indestructible as its dispersion. But, if we have advanced versions of Blockchain in future then this problem would be diluted.

ACKNOWLEDGMENTS

I would also like to express my special thanks to Dr. Jawed Ahmed, Associate Professor Computer Science, my Supervisors at Jamia Hamdard University, New Delhi for his insight and knowledge on the subject, who imbued me with the feeling to work assiduously.

Finally, I take this opportunity to thank my parents, family members and friends for their moral support and help and extended thanks to my well wishers

REFRENCES

[1] Nir Kshetri, "Can Blockchain Strengthen the Internet of Things?," IT Professional, vol. 19, no. 4, pp. 68 - 72, May 2017, Available: http://ieeexplore.ieee.org/document/8012302/

[2] Mahdi H. Miraz, "Blockchain: Technology Fundamentals of the Trust Machine," Machine Lawyering, Chinese University of Hong Kong, 23rd December 2017, Available: http://dx.doi.org//10.13140/RG.2.2.22541.64480/2

[3] Don Tapscott and Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 1st ed. New York, USA: Penguin Publishing Group, 2016.

[4] Maaruf Ali and Mahdi H Miraz, "Cloud Computing Applications," in Proceedings of the International Conference on Cloud Computing and eGovernance - ICCCEG 2013, Internet City, Dubai, United Arab Emirates, 2013, pp. 1-8, Available: http://www.edlib.asdf.res.in/2013/iccceg/paper001.pdf

[5] OECD. Health spending. 2018. doi: https://doi.org/https://doi.org/10.1787/8643de7e-en. URL https://www.oecdilibrary.org/content/data/8643de7e-en.

[6] Elizabeth A Bell, Lucila Ohno-Machado, and M Adela Grando. Sharing my health data: a survey of data sharing preferences of healthy individuals. In AMIA Annual Symposium Proceedings, volume 2014, page 1699. American Medical Informatics Association, 2014.

[7] Dr. Fabian Wahl Peter Behner, Dr. Marie-Lyn Hecht. Fighting counterfeit pharmaceuticals, 2018(accessed Nov 15, 2018). https://www.strategyand.pwc.com/reports/counterfeit-pharmaceuticals.

[8] Tsung-Ting Kuo, Hyeon-Eui Kim, and Lucila Ohno-Machado. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association, 24(6):1211–1220, 2017. doi:

10.1093/jamia/ocx068. URL http://dx.doi.org/10.1093/jamia/ocx068.

[9] Vikram Dhillon, David Metcalf, and Max Hooper. Blockchain in Health Care, pages 125–138. Apress, Berkeley, CA, 2017. ISBN 978-1-4842-3081-7. doi: 10.1007/978-1-4842-3081-7_9. URL https://doi.org/10.1007/978-1-4842-30817_9.