Relative Importance of Blockchain in Health Care: Enhancing data sharing and mitigating cyber security crimes

HARI PRIYA PONNAKANTI, University of Cincinnati, United States
MURAT OZER, University of Cincinnati, United States
BILAL GONEN, University of Cincinnati, United States

This paper looks at the opportunities and challenges of implementing blockchain technology across medical sector and provides a clear view which can enable blockchain for more extents. After a notable research on underlying blockchain technology which offers distributed governance, immutable audit trail, provenance of data, robustness and privacy, we contrasted blockchain innovations and identified prominent applications of it in historically decentralized healthcare sector. As healthcare industry faces many challenges like unauthorised data sharing, lack of data transparency, ransomware, data breaches and cyber crimes, blockchain is one of the best way to enhance data sharing and to mitigate prominent cyber crimes. By proper designing of a decentralized and immutable blockchain network where the data is dispersed among credentialed social insurance experts guarantees that cybercriminals cannot touch single patient's confidential data, which facilitates encryption or cryptography of personal data where no patient's emergency data is at extreme hazard. Blockchain trust-worthy cloud is one of the most powerful and secured way of storing high confidential data. After analysing Blockchain implementations and identifying its potential in healthcare, we conclude with several promising directions for future research.

CCS Concepts: • **Information systems → Distributed storage**.

Additional Key Words and Phrases: Blockchain, Potential Optimization, Distributed ledger technology, Decentralized Networks, Interoperability

ACM Reference Format:
Hari Priya ponnakanti, Murat Ozer, and Bilal Gonen. 2020. Relative Importance of Blockchain in Health Care: Enhancing data sharing and mitigating cyber security crimes . In *IT Research Symposium '20: School of Information Technology IT Research Symposium, April 14, 2020, Cincinnati, OH, USA.*https://scholar.uc.edu/

1 INTRODUCTION

Blockchain technology is mostly referred as groundbreaking innovation, kind of indicator to new economic era. Blockchain might came into global market as a new form of economic system [2], but it is essential for recording every digital event and however this data is not just recordings, it also contains smart information that are stored in the programs of the blockchains [15]. Blockchain comes with solving serious issues in the current business market by replacing centralized architectures with decentralised and secured ones, where even third-party organizations should verify themselves [15]. Blockchain ought to be considered as a dispersed affix just timestamped information structure. One study over conceptual proposal on blockchain is the idea of using trade credit as the value of transactions, and this trade credit is in the scope of trade secret which improves trade confidentiality and makes it more secure[7]. Speaking of blockchain in Healthcare sector, normally the medical data and its backup records are housed in the traditional medical institution where the data can be maliciously manipulated, and it is difficult to share between different institutions. These

IT Research Symposium '20, April 14, 2020, Cincinnati, OH

can be mitigated by using blockchain techniques like Blockchain Bitcoin,cryptography, distributed blockchain ledger. Blockchain had got best features like decentralization, cryptographic security and immutability to make a strong contender that can reshape the healthcare landscape all around the world and make it hard for the criminals to hack or breach the data[10]. In this paper, we dealt with all the aspects starting from the challenges that healthcare industry is facing, till presenting the appropriate solutions for enhanced data sharing and reduced cyber security crimes.

2 CHALLENGES IN HEALTHCARE INDUSTRY

As we mentioned about the prominence of blockchain precisely, in 2014 US Department of Health and Human Services went through a rough weather when almost 16 million people's medical information was compromised and was stolen from all the health care providers. Such cases are usually called as theft and hacking the data. One of the main reasons for cyber-attacks on healthcare departments is investing very less amount on securing the medical data or the personal data. According to Symantec, every leading security vendor healthcare organizations are so particular about limited investments on security[3]. And according to the Federal Bureau of Investigation, electronic health records (EHR) were recorded as more valuable compared to financial data when EHR's can be sold at 50 dollars in the black market compared to a stolen social security number which is hardly bought by 1 dollar or even a credit card number. It is difficult to disregard the increasing ransomware attacks on health clinics.

Ransomware has become such an issue, that the MS-ISAC, alongside the accomplices at the National Health Information Sharing and Analysis Center (NH-ISAC) and Financial Services Information Sharing and Analysis Center (FS-ISAC), collaborated to have trainings around the nation on the best way to shield against it[8]. Ransomware is a kind of malware that contaminates frameworks and documents, rendering them distant until a payoff is paid. At the point when this happens in the medical services industry, basic procedures are eased back or turn out to be totally inoperable. Usually ransomware will be infecting victim's machine in 3 ways such as user clicking on a malicious link, and through phishing emails that contains several malicious attachments and finally by encountering any phishing advertisements that contains malware.

Associations are regularly excessively engrossed with shielding the integrity of their organization and system from outer dangers to address the genuine and perilous hazard that may exist in their own association – insiders[4]. Where the insiders can genuinely access restrictive frameworks with no limits confronting from customary cybersecurity resistances, like, intrusion discovery gadgets or physical security and will have good idea on system arrangement and vulnerabilities[4]. The insider risk can be caused from: those accidentally tapping on a pernicious connection or losing a work gadget containing delicate information to those who intentionally selling PHI/PII for personal benefits. Data breach- this is one of the most prominent challenge faced by a healthcare industry, it is a cybersecurity error in which private or critical information is copied and stolen from the company may then be used for financial profit and damage in a number of ways. Therefore, there is a higher incentive for cyber criminals to target medical databases, so they can sell the PHI or use it for their own personal gain.

3 APPLICATION OF BLOCKCHAIN TECHNOLOGY IN HEALTHCARE

Blockchain is generally treated as a distributed ledger for distributing, storing, evaluating, documenting, and validating purposes among stakeholders in the health care industry[14]. Such implementations can be further classified depending on their main goals of leveraging blockchains. Most researches or ongoing projects concentrate on sharing information on patient care using blockchains to strengthen the monitoring of medical records,information approval, evaluation, authorization, improved insurance benefits, streamlined clinical research, system and software

gateways to health care. Blockchain is permitting to record genomics information that can battle fake pharmaceuticals and ensure licensed innovation rights [11]. Medicinal Genomics Corporation is an atomic data organization that applies best in class life science innovation to Cannabis plant hereditary qualities and committed to sequencing of genomes of the patients with seizure issue, where it stores all that genomic data on is decentralized blockchain administration[3]. Blockchain is appropriate for applications those autonomously oversaw biomedical/medicinal service partners with high information provenance e.g., emergency clinics, suppliers, patients, and payers who wish to work together with each other by following the cryptographic conventions [12]. The last key advantage of blockchain is identified with the improved security and protection utilizing cryptographic calculations. For instance, Bitcoin blockchain uses the 256-piece Secure Hash Algorithm (SHA256), a cryptographic hash work characterized in the US Federal Information Processing Standards 186-4, distributed by the National Institute of Standards and Technology, as the cryptographic hash work in the hash-chain that the confirmation of-work calculation runs on. SHA-256 is likewise used to produce client addresses for security/obscurity improvement i.e., every client is spoken to by a hash an incentive rather than a genuine character, for example, an IP address.

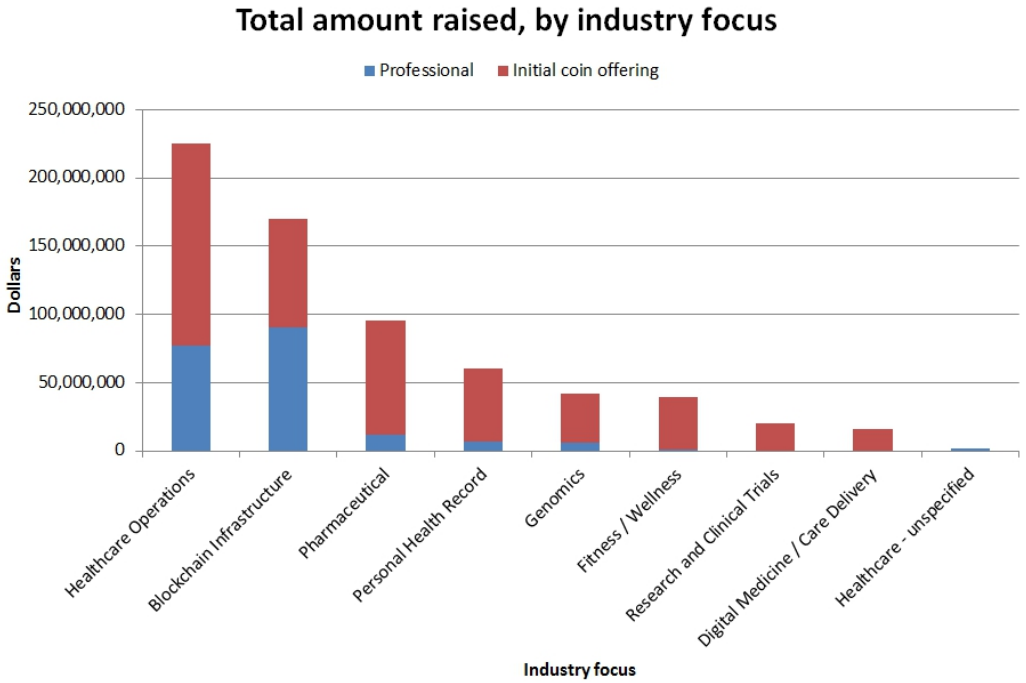

Fig. 1. Blockchain market capitalisation in Healthcare industry[5]

The blockchain-based, distributed innovation will computerize assortment and sharing of genomic information to some degree by enabling people to transfer their own DNA profiles control which scientists may access and add to each protected store of data [3]. This could be a stage where genomic data stored properly. Blockchain ledger helps Food and Drug Administration (FDA) licenses to become quicker in new drug innovation methods due to different data collection, audit trail supply chain screening and reduced theft due to the acknowledgment of different network events. In terms of data inviolability and historicity, blockchain guarantees that incidents are

recorded in their proper chronological order, effectively preventing a post-reconstruction study[1]. Firstly, the cryptographic verification of each transaction guarantees information integrity. This is crucial to maintaining data integrity — preventing information falsification, data "beautification" and software innovation in some way[9]. Secondly, traceability and data historicity are among the core features of the technology: every transaction with Blockchain is timed. Such material is freely transparent; a copy of the time-stamped data evidence is held by any client. And thirdly immutable audit trail and data security, where all the critical information is stored in an unchangeable ledger record and high privacy using cryptographic algorithms .

From the fig.1, we can clearly review how various sectors of healthcare industry are pouring huge amount of money in blockchain technology. We described the key benefits and comparative advantages of blockchain technology in various healthcare domains like healthcare genomics, pharmaceuticals, clinical research and biomedical in order to better understand why distributed ledger technology can be feasible for health applications[1].

4 BLOCKCHAIN FOR ENHANCED DATA SHARING IN HEALTHCARE INDUSTRY

The potential for the utilization of blockchain innovation in medical clinics has begun to be tried in a few pilot extends in an inclusive way. A year ago, in the United States, Booz Allen Hamilton Consulting created and executed a blockchain-based pilot stage, intended to support the Food and Drug Administration and Office of Translational Sciences where they investigated how to utilize it as an innovation for medicinal services and use the information for the executives[3].

The pilot venture is as of now being utilized at four significant medical clinics; it is utilizing Ethereum to oversee information get by the means of virtual private systems. The venture is based on the IPFS to use encryption and diminish information duplication by means of off-chain cloud parts with cryptographic calculations to make client sharing. On one hand, blockchains appear to speak to a decent arrangement with GDPR (with regards to information convenience,information discernibility and legitimate access auditability)[13]. There are some issues those may debilitate the real power of information, through programmed execution. One choice to handle these issues is 'dynamic assent the executives', which is completely in accordance with the GDPR arrangement regarding assent. Moreover, it is viewed as that 'private blockchains', e.g., Enterprise Blockchain can without much of a stretch consent to GDPR mandates since the exchanges of the advanced records of the put away data can be altered and deleted by private substances or specialists who can possess and control this stage, utilizing a specific class of agreement calculation[1].

The organization '23andMe', which was established in 2006, is the most productive, offering direct-to-purchaser hereditary testing administrations[10]. As security is a significant issue in the human services industry, a year ago, 23andMe reported that they had sold a USD 300 million stake in the organization to the pharmaceutical monster GlaxoSmithKline, viably giving over access to the 5 million clients' information, despite it just containing exome information[13]. To address such future concerns,new companies are using blockchain for social insurance guarantee to offer an answer for buyers needing to have a DNA test done, by keeping information possession. Present day blockchains are on a very basic level transparent platforms where communications among clients and Smart Contracts, displayed by cryptographically marked yet decoded transactions, are visible to each member on the blockchain network[11]. This focal element of blockchain innovation brings about evident difficulties to actualizing arrangements that share sensitive information, where just are stricter number of beneficiaries ought to be given access to a bit of information, or a cryptographic artifact that can open a bit of data-store off the blockchain. Considering this, blockchain must be implemented along with a well designed software to encourage extra layers of encryption that uphold the protection of substance inserted inside exchange information. To empower information sharing across hospital frameworks, we can develop purpose-fabricated

arrangement dependent on hospital privacy and security prerequisites that use an assortment of solid cryptographic algorithms to enable user and bunch based secret sharing. To construct an information sharing framework requires additional plan prerequisites including the utilization of halter kilter cryptographic algorithms and approaches to facilitate encryption and decryption operations on arbitrary data. Algorithms utilizing uneven cryptography use open and private keys to decode information [6]. The keys are basically huge numbers that have been matched together yet are not indistinguishable. Since file storage is decentralized, and has a huge potential assault surface, all information is completely scrambled before being composed into it. Since information is stored within an outer stockpiling arrangement, the blockchain segment of our framework is mindful for executing Smart Contracts that, in part, refer to our information and give data on how information is possessed, recovered, and decoded [13].

5 HOW CAN WE MITIGATE CYBER SECURITY CRIMES IN HEALTHCARE BY USING BLOCKCHAIN TECHNOLOGY?

Healthcare industry flows out with a constant barrage of cyber-attacks, and it is also known that healthcare industries experiences twice the rate of phishing emails and cyber-attacks compared to other industries. Every day new challenges arise, and cyber-attacks are also learning new phases where the phishing data is totally encrypted and could sometimes be very hard to decrypt. Blockchain could be the gravely required answer for an issue that puts patients and emergency clinics at extreme hazard. The DLT's decentralized state permits just certain people to have limited quantities of data that, whenever consolidated, would include a patient's whole well being diagram. The dispersion of just certain data to credentialed social insurance experts guarantees that cyber criminals can't get to every single recognizable part of a person's well-being record.

Usually healthcare industries now-a-days are trying to working hard to get the data under more secured stage and to protect the data server at whatever the cost it could end up, but by taking the data storage levels to such locations where no other security detail can breach in would help the data to be more secured. For example, Data of Google is held at a very secure location in the middle of the ocean where it is not wired with any other network and due to that hacking into those systems is really a tough call for any phishing mails or even a hacker. The insider attacks-these attacks from insiders of the organizations can be mitigated by storing all the sensitive and confidential data in a specific blockchain repository with only access to official members of the organization and educating the members and employees about how to detect and notify an insider attack or avoid them from unwittingly being one. And coming to the most important cyber security issue, Data Breach, this can be reduced by designing a decentralized and immutable network which facilitates encryption or cryptography of personal data[3]. It is critical that cryptography is carried out at rest and in transit, and that third parties and stakeholders who also have access to your healthcare infrastructure or directories also treat patient data appropriately. The laws like Federal HIPAA Security Rule works on protecting Electronic Health Records(EHR). Moreover, hackers can only break into conventional networks and find all the data in a single repository and exfiltrate or corrupt it, but the blockchain makes this impossible [4]. The data is decentralised, secured and cross-checked across the entire network. Once the record is on the ledger, it's almost impossible to change or delete it without finding it and invalidating the signature. Each valid transaction is confirmed by multiple network nodes. To effectively hack blockchain, you'd have to hack most of the nodes simultaneously, which, while technically possible with enough super-computing capacity and resources, is far beyond the skill of cyber criminals today.

6 CONCLUSION

In the medical information sharing system, we combine the knowledge of blockchain, database and cryptography to build a system for the sharing of medical information. By using the system, we can improve the use of medical data and encourage the sharing of medical data. It will be of great benefit to the development of medicine. In addition, the clinical data digest encode requires the support of health professionals. Blockchain technology cannot prevent information from falling into the wrong hands, but it can provide a high degree of surety that the entity accessing it is who they claim to be. As a result, companies can store records and other digital objects on a distributed ledger in the confidence that they will always be available and virtually impossible to delete. Through eliminating much of the human element from data storage, blockchains greatly mitigate the risk of human error, which is the main cause of data breaches. It is technology that always drives science forward. Blockchain technology is a type of system needed to achieve the next order of magnitude of change in vital areas such as human health / genome science, agriculture, pharmacy and beyond. So far, blockchain technologies have made a great difference in Bitcoin and in Banking sector and such differences we are going to see in Healthcare Industry or Healthcare applications and few benefits are to improve medical record management, enhance the process of insurance claim and clinical & biomedical research data ledgers. Blockchain distributed ledger protocols can advance the healthcare and biomedical domains in all possible ways and it is also known that there are more and more advanced applications are yet to emerge soon.

REFERENCES

[1] A Acikgoz and F Apak. 2019. A Conceptual Proposal on Blockchain: Distributed ledger of corporate liquidity. *Journal of Yaşar University* 14, 53 (2019), 31–41.

[2] Roman Beck, Christoph Müller-Bloch, and John Leslie King. 2018. Governance in the blockchain economy: A framework and research agenda. *Journal of the Association of Information Systems* 19, 10 (2018), 1020–1034.

[3] L. N. Chavali, N. L. Prashanti, K. Sujatha, G. Rajasheker, and P. B. Kavi Kishor. 2018. The emergence of blockchain technology and its impact in biotechnology, pharmacy and life sciences. *Current Trends in Biotechnology and Pharmacy* 12, 3 (2018), 304–310.

[4] CISblog. 2019. Cyber Attacks: In the Healthcare Sector. https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/

[5] ANDY CORAVOS and NOAH ZIMMERMAN. 2019. Blockchains for biomedicine and health care are coming. Buyer: be informed - STAT.

[6] Marek A Cyran. 2018. Blockchain as a foundation for sharing healthcare data. *Blockchain in Healthcare Today* 1 (2018), 13.

[7] Andy Extance. 2015. The future of cryptocurrencies: Bitcoin and beyond. *NATURE* (oct 2015), 21–23.

[8] Ryan Fahey. 2020. Top Cyber Security Risks in Healthcare. https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-cyber-threat-landscape/top-cyber-security-risks-in-healthcare/#gref

[9] Yi Fang, Linhu Cong, Jianqiu Deng, Weixin He, and Yuliang Chen. 2019. Research on Application of Missile Blockchain Based on Nation Secret Algorithm. *Journal of Physics: Conference Series* 1237, 2 (jun 2019), 022–138.

[10] Antonia Ferrer-Sapena and Enrique-Alfonso Sánchez-Pérez. 2019. Applications of blockchain technology in scientific documentation: current situation and perspectives. *El Profesional de la Información* 28, 2 (mar 2019), 12.

[11] William J Gordon and Christian Catalini. 2018. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Computational and structural biotechnology journal* 16 (2018), 224–230.

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

[13] Claudio Lima. 2018. Blockchain GDPR privacy by design. *IEEE Blockchain Group* 4 (2018), 5.

[14] Harlan M Krumholz Suveen Angraal and Wade L Schulz. 2017. Blockchain technology: applications in health care. *Circulation: Cardiovascular Quality and Outcomes* 10, 9 (2017), e003800.

[15] Zibin Zheng, Shaoan Xie, Hong Ning Dai, Xiangping Chen, and Huaimin Wang. 2018. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services* 14, 4 (2018), 352–375.