TO STUDY THE APPLICATION OF BLOCKCHAIN IN STRENGTHENING ELECTRONIC HEALTH RECORDS

Dissertation Submitted to

The IIHMR University, Jaipur

For the partial fulfillment

for the award of the degree of Master of Business Administration

(MBA) In

Hospital and Health Management

By

Aditya Singh

Under the Supervision and Guidance of

Dr. Arindam Das

2021

TO STUDY THE APPLICATION OF BLOCKCHAIN IN STRENGTHENING ELECTRONIC HEALTH RECORDS

Dissertation Submitted to

The IIHMR University, Jaipur

For the partial fulfillment

for the award of the degree of Master of Business Administration (MBA) In

Hospital and Health Management

By

Aditya Singh

Under the Supervision and Guidance of

Dr. Arindam Das

2021

DECLARATION BY STUDENT

I hereby declare that this dissertation titled 'To study the application of blockchain in strengthening electronic health records' is the bonafide record of my original research work. I declare that it has not been submitted to any other university or institution for the award of any degree or diploma. Information derived from the published or unpublished work of others has been duly acknowledged in the text.

Name of Student: Aditya Singh

Date: 30/06/2021

CERTIFICATE

This is to certify that Aditya Singh in partial fulfilment of the requirements for the award of the degree of MBA (Hospital and Health Management) from IIHMR University, Jaipur has successfully completed his internship at Clarivate- Medtech Insights from 1st Febraury 2021 to

Place : Preceptor/Head of the organization

Date Name of the Organization

CERTIFICATE

This is to certify that dissertation titled 'To Study Application of Blockchain In Strengthening Electronic Health Records' is a record of the research work undertaken by Aditya Singh in partial fulfillment of the requirements for the award of the degree of MBA (Hospital and Health Management) from the IIHMR University, Jaipur under my guidance and supervision and his/her approach to the research study has been sincere, scientific, and analytical.

Faculty Guide	School Dean
IIHMR University, Jaipur	IIHMR University, Jaipur
Date	Date

ACKNOWLEDGEMENT

Learning is a never ending process. Our quest to learn more and more by grabbing every possible opportunity that comes our way, proves to be the reason behind our success one day.

I would like to thank the management for providing me with this learning opportunity which has enhanced my knowledge related to blockchain based solution for strengthening electronic health records. Working on this report has made it possible for me to explore the topic in all possible dimensions to extract best out of all the data available and turn this opportunity into a beautiful learning experience.

My sincere thanks to my mentor **Dr. Arindam Das** who has been a constant support and has guided me in the correct direction throughout my learning process.

My heartfelt gratitude and appreciation are also extended towards **Dr. Sangeetha Iyer** (Organization-Mentor) and **Mr. Ashish Bhupal** (Organization-Manager) for their useful advice and constant support in the completion of my project report.

Lastly, I admit my inability to express my emotions through words for my loving parents and for their encouragement, support and constant faith in me.

Above all I thank the Almighty for giving me patience and strength to overcome the difficulties, which crossed my way in accomplishment at this endeavour.

Abstract

Title- Blockchain based solution for Electronic Health Records

In the present era of smart cities and homes, the private information of the patients such as their names, address, and disease is being breached on a regular basis, which indirectly related to the security of electronic health records (EHRs). The existing state-of-the-art schemes handling the security of EHRs have resulted in data being generally inaccessible to patients. These schemes struggle in providing the efficient balance between the data privacy, data security, interoperability, need for patients, and providers to regularly interact with data. Blockchain technology resolves the aforementioned issues because it shares the data in a decentralized and transactional fashion. This can be leveraged in the healthcare sector to maintain the balance between privacy and accessibility of EHRs. s. In this paper, we propose a Blockchain-based framework for efficient storage, privacy and security of data for the maintenance of EHRs. The goals of this paper are to analyze how blockchain works and how blockchain helps in strengthening of EHRs.

Objectives-

- To understand the technology of Blockchain and how does it work.
- To study the application of Blockchain to strengthen Electronic Health Record.

Methodology-

The report is based on the descriptive secondary research data. Previous articles regarding, blockchain and role of blockchain in electronic health records were reviewed and data was collected from them. Articles pertaining to structure of blockchain were also reviewed to understand its structure.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

With each passing year, technology grows more entwined with ordinary life and it is gradually expanding into the health-care sector. Many developing nations are progressively using EHRs. Due to the projected benefits, many governments have expressed interest in utilising EHRs; for example, the United States government decided in 2004 that by 2014, most Americans would be connected to EHRs. Later, as part of the American Recovery and Reinvestment Act of 2009, a total of $19000 million was set aside to be utilised in digitalizing health care records in the United States. Similarly, according to the High Level eHealth Conference conducted in 2010, the European Union nations aimed to have a single health system in place by 2015. The European Union's goal is to share patient electronic health record data in order to provide high-quality, cost-effective health care.

What is EHR?

"An electronic health record (EHR) is a digital version of a patient's medical chart that is maintained by the provider over time and may include all of the key administrative clinical data relevant to that person's care under a particular provider. Integrating evidence based medicine into the EHR allows health professionals to better manage patient care through electronic health record (EHR) systems. Many EHRs are also designed to provide information to the patient and to share information with other health care providers. An EHR contains valuable and pertinent automated medical information, including: Patient vitals, prescriptions, medical histories, diagnoses, surgical notes, discharge summaries."

-Source: Health IT.gov, NCBI, NIH

In the past, a medical record was information written down for scientific, therapeutic, administrative, and financial purposes. Its primary shortcoming was in terms of accessibility and it was accessible to one person at a time. Because it was updated manually, it took anything from 1 to 6 months or more to complete. EHRs have many advantages over paper records in terms of – reduced adverse drug reaction because EHR are connected to pharmacies and drug banks, accessibility of data, large amount of data can be stored, reduce the chances of losing records and data can facilitate research

activities. The office of the NCHIT refers to the health record as "not just a collection of data that you are guarding, it is life." The information in the record belongs to the patient. The physical medical record belongs to the physician and the organisation. However, the emergence of EHRs has raised worries about healthcare data security.

Data breaching of patients name, address, disease etc is something which questions the security of electronic health records. Despite its rising utility and growing enthusiasm for its adoption, the ethical considerations that may arise are receiving little consideration. Security, privacy, interoperability and confidentiality are potentially major problems in EHRs. Only with the patient's agreement or as authorised by law can information about a patient be shared with others. When a patient is unable to make judgments about releasing information owing to age or mental incompetence, such decision should be made by the patient's legal representative or legal guardian. The key to maintaining secrecy is to limit access to information to only those who are authorised. The first step is to authorise users. Many existing EHR systems employ a centralised server paradigm, as a result such deployments inherit the centralised server model's security and privacy constraints.

What is blockchain?

"A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT)."

-Source: Bocconi University

Blockchain technology has emerged as a strong technology capable of providing distributed storage with immutability, secrecy, and user access features. Blockchain exchanges data in a decentralised and transactional manner, hence overcomes the aforementioned difficulties.

"Blockchain was invented by a person (or group of people) using the name Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency bitcoin. The identity of Satoshi Nakamoto remains unknown to date. The invention of the blockchain for bitcoin made it the first digital currency to solve the double-spending

problem without the need of a trusted authority or central server. The bitcoin design has inspired other applications and blockchains that are readable by the public and are widely used by cryptocurrencies. Blockchains are typically managed by a peer-to-peer network for use as a publicly distributed ledger, where nodes collectively adhere to a protocol to communicate and validate new blocks."

-Source: Wikipedia

According to Accenture, a study of the diffusion of innovations theory found that blockchains were adopted at a rate of 13.5 percent in financial services in 2016, putting them in the early adopter stage.

The WSG stated that E&Y was developing on a blockchain to enable companies, governments, airlines, and others monitor those who have undergone antibody testing and may be resistant to the COVID-19 pandemic in 2020. Blockchain was also used by hospitals and vendors to track essential medical equipment.

"Blockchain is divided into three categories. The 1st generation – In 2009, blockchain 1.0 was released, and it relied on hardcoded special-purpose systems to focus on digital money and served potentially malicious public participants. The 2nd generation – Blockchain version 2.0 was started in 2014 and it found innovative ways of application of smart contracts for different scenarios with the help of Etherium blockchain technology. Blockchain version 3.0 started in 2017 with hyperledger. It helped in providing an all-purpose permissioned decentralized application system, mostly associated with user-friendly and highly configurable features. "

-Source: The Science and Information Organization

Significant systems in logistics, certifications, and banking were built in the second generation of blockchain. Education, health, agriculture, the Internet of Things (IoT), and governance Smart Grid, Intelligent Transportation System, Data Center Networking, Electronic Voting System, and more domain applications have recently been included. To establish the normalcy of blockchain technology, all three have assisted one another.

TYPES OF BLOCKCHAIN

"Current blockchain systems are categorized into four types: public, private, consortium and hybrid blockchains. They are:

Public Blockchains: Public blockchains provide a fully decentralized network, where every member can access the blockchain content and could take part in the consensus process (e.g. Bitcoin and Ethereum).

Private Blockchains: Private blockchains are dedicated for single enterprise solutions and utilized to keep track of data exchanges occurring between different departments or individuals. Every participant need consent to join the network and considered as a known member once it has been adhered.

Consortium Blockchains: A consortium blockchain is a permissioned network and public only to a privileged group. It is used as an auditable and reliably synchronized distributed database that keeps track of participant's data exchanges.

Hybrid Blockchains: Hybrid blockchains combine the benefits of private and public blockchains. Therefore, a public blockchain is employed to make the ledger fully accessible, with a private blockchain running in the background that can control access to the modifications in the ledger."

-Source: Springer Link

RATIONALE

With the advancement of technology and growing consumerism, it is important to evaluate how we can benefit from these emerging technologies such as blockchain to ensure the process of transparency and leverage trust in order to enhance the value proposition. The study aims to find about the applications of blockchain in strengthening the electronic health records.

RESEARCH QUESTION

What are applications of blockchain based solutions to strengthen electronic health records?

RESEARCH OBJECTIVES

- To understand the technology of Blockchain and how does it work.
- To study the application of Blockchain to strengthen EHR.

METHODOLOGY

Research Design- Systematic Literature Review

Data collection tool- Information was searched across analyst commentary, journals, thought leadership papers, blogs, news articles and published studies in order to collect the material which is available online to provide a comprehensive understanding of the following parameters-

- Understand the technology of blockchain and how does blockchain work?
- Blockchain based solution to strengthen EHRs

Keywords searched- Blockchain, EHR, Security, Privacy, Interoperability, Challenges, Smart Contracts

Inclusion criteria- Any information that discussed about what blockchain is, how does it work and challenges related to privacy, security, interoperability and immutability in EHR.

Exclusion criteria- Articles before 2014 were not included in the study

Duration of the study- 3 months

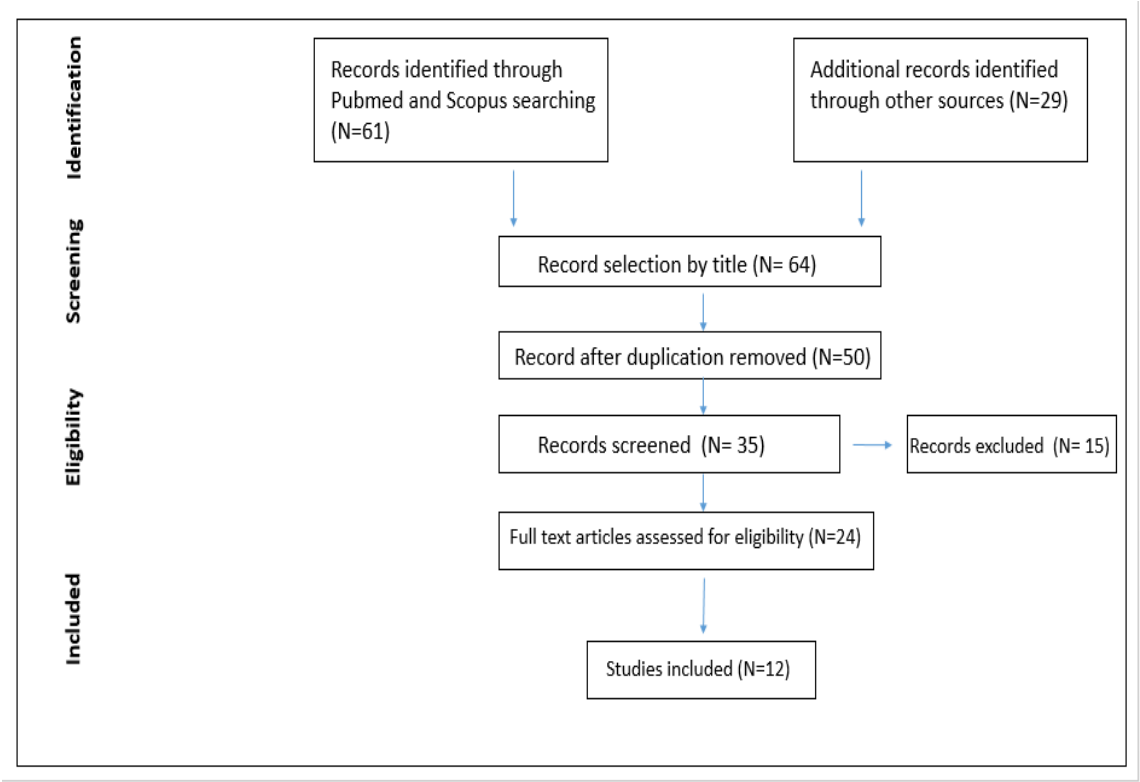

Figure 1: Flow diagram depicting the search process

LITERATURE REVIEW

Literature 1:

"Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in clinical research*, *6*(2), 73–76. https://doi.org/10.4103/2229-3485.15399"

The study was undertaken by Amit Sharma, Praveen Aggarwal, Fouzia F. Ozair and Nayer Jamshed. The objective of this study is to understand the benefits and ethical issues in EHRs. The study was conducted in India. In the study they found many benefits of EHR such as – reducing the problem of wrong prescriptions, doses and procedures by producing legible records in EHR. When EHR's are connected with pharmacies and drug banks it reduced adverse drug reaction events. EHR requires less storage space and can be stored for an infinite period of time. EHRs help with research,

give a full collection of backup records for a low price, speed up data transfer and are cost-effective. Two events of security breaches took place in the year 2013 at Howard University Hospital where patients' diagnosis related information, social security numbers, names, addresses and Medicare numbers for more than 34,000 patients were compromised. Loss and destruction of data also occurs during data transfer which leads to inaccurate information being sent to insurance companies. According to the findings of the study EHR capacity must be utilised in order to improve the safety, efficiency, quality and effectiveness of healthcare delivery systems.

Literature 2:

"Ismail Keshta, Ammar Odeh, Security and privacy of electronic health records: Concerns and challenges, Egyptian Informatics Journal, Volume 22, Issue 2, 2021, Pages 177-183, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2020.07.003."

The study was conducted by Ismail Keshta and Ammar Odeh. The objectives of the study were- (1) to address concerns about EHR privacy and security (2) advantages of EHR (3) IT security incidents in health care settings. They discovered that EHRs are more successful and offer more advantages, such as decreasing costs, increasing health care quality, supporting the use of evidence-based medicine, assisting in record keeping and ensuring record portability. Privacy, security, and confidentiality are all problems that must be handled in an electronic medical record system. Privacy of personal health records was a matter of concern for 66% of clients and only 40% of the clients felt that health data was secure and safe. There were some concerns related to health information privacy such as patients refusing to disclose their personal information to health care providers, giving wrong patient personal information to medical institutions and demanding the removal of patient personal information. At least one security breach affected less than 500 patient's data which was reported in 21% of healthcare providers. 68% of the healthcare organizations that were surveyed in US reported that they had recently experienced a significant security incident which comprised of security incidents from insider and external threats. They found in the study that EHR security and privacy issues are critical, based on the fact that if sensitive information is revealed to a third party, the patient may suffer significant consequences.

Literature 3:

"Ayanthi Jayawardena, A systematic literature review of Security, Privacy and Confidentiality of patient information in Electronic Health Information Systems, Sri Lanka Journal of Bio-Medical Informatics,2021, DOI: 10.4038/sljbmi.v4i2.5740"

The study was undertaken by B. A. Saranga Jayawardena. The study aims to understand the problems related privacy, security and confidentiality of patient information related to EHRs. Unauthorized access to EHRs, unauthorised exposure of sensitive data, possible fraud from data and data tampering were all cited as important privacy and security concerns in the research. The majority of patients were concerned about their EHRs' privacy and security, although many thought that the advantages of EHRs outweighed the risks. The paper also discussed instances in which the privacy of mental health databases was violated. Genetic/genomic test results should be treated differently than other medical data since they contain highly individualised information, which should be secured to maintain patient's trust. Security, privacy, and confidentiality were highlighted as key issues with EHRs. None of them were 100% secure and only two (8%) were Health Insurance Portability and Accountability Act (HIPAA) compliant.

Literature 4:

"McDermott, D.S., Kamerer, J.L., & Birk, A.T. (2019). Electronic Health Records: A Literature Review of Cyber Threats and Security Measures."

The study was conducted by Donna S. McDermot, Jessica L. Kamerer and Andrew T. Birk. The study was conducted in USA. The study aims to educate and inform the cyber security threats and attacks taking place in EHR's. The potential threat categories were categorized as – administrative, technical, physical, insider use and portable devices. Despite the efforts made by the government to safeguard EHR it is being targeted by cyber-criminal. In 2015 there were 187 reported breaches which comprised of personal information of 84 million patients. 21% of all cyber security breaches worldwide accounted for healthcare breaches. New methods and security concerns of stealing private health information have evolved over the years. Healthcare industries do not

invest in developing cyber security measures compared to other industries like retail or banking. This is the reason why there has been an increase in targeting and vulnerability to cyber threats.

Literature 5:

"Khin Than Win, A Review of Security of Electronic Health Records, The HIM journal 34(1):13-8,2015, DOI: 10.1177/183335830503400105."

The study was undertaken by Khin Than Win. The study's goal was to see if existing information security methods are sufficient for EHRs. Several security breach events were reported in the article-(1) patient records being exposed on the internet (2) patient name of 4000 HIV positive patients sent to Florida newspapers (3) A hacker gained access to the University of Washington Medical Center's computer system and stole information of 5000 cardiology and rehabilitation medicine patients. (4) The identities of dead kidney donors were accidentally released by the University of Minnesota. According to the findings of the study, current information security solutions are still insufficient, and EHR security may still be improved.

Literature 6:

"Reisman M. (2017). EHRs: The Challenge of Making Electronic Data Usable and Interoperable. *P & T : a peer-reviewed journal for formulary management*, *42*(9), 572–575."

The study was conducted by Miriam Reisman. The objective of the study was to understand interoperable challenges in EHR. There are several government-certified EHR solutions in use across their country, each with its own set of technical standards, functional capabilities, and clinical terminology. Due to these differences creating a standard interoperability format for sharing the data is difficult. EHR systems are frequently heavily tailored to an organization's particular workflow and preferences, they are not always compatible when developed on the same platform. When two EHR systems are able to share information and use data, they are considered to be interoperable. The research found that the future of EHR and its capacity to be an essential tool in care coordination and team-based care would be determined by the actions done by EHR vendors and the federal government to guarantee interoperability is a top priority.

Literature 7:

“J. Vora et al., "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1-6, doi: 10.1109/GLOCOMW.2018.8644088.”

The study was undertaken by Sudhanshu Tyagi, Jayneel Vora, Sudeep Tanwar, Anand Nayyar, Joel Rodrigues and Neeraj Kumar. The goal of this research is to learn more about the proposed blockchain-based strategy for EHR storage, data transmission, and privacy and security. According to a study of healthcare stakeholders, 16 percent expect to utilise a blockchain-based solution in the near future, with 56 percent planning to do so by 2020. Blockchain can be used in – medical claims/billing management, medical research, securing patient’s data and drug supply chain. According to the findings, unauthorized access by diverse players is further reduced and a sense of decentralisation is produced by combining specific nodes with improvised authority. Although it is very improbable to entirely hide all information while maintaining an accessible and interoperable system, the suggested framework nevertheless provides substantial privacy and data integrity by utilising smart contracts to segregate information.

Literature 8:

“Alam, S.; Ahmad Reegu, F.; Daud, S.M.; Shuaib, M. Blockchain-Based Electronic Health Record System for Efficient Covid-19 Pandemic Management. Preprints 2021, 2021040771 doi: 10.20944/preprints202104.0771.v1”

The study was conducted by Shabad Alam and Mohammed Shuaib. The objective of this study is to understand issues with EHR systems and use of blockchain to resolve these issues. They found that if precautions have not been taken to protect the EHR, it becomes easy to hack it. Electronic health records contain highly crucial and critical patient-related medical data, requiring safe storage, sharing, retrieval, and scope. Blockchain can be used to improve and modernise electronic health record exchanges by delivering a secure approach for exchanging medical data by safe guarding it through peer-to-peer linkage. Blockchain technology has the advantages of improved patient information access, interoperability, security, privacy and immutability. When blockchain is combined with IoT and cloud computing it tends to give better EHR

solutions. Medical history of any patient is easily accessible which reduces the chances of wrong drug prescription. Their findings show that Blockchain is a technology that can be efficiently used to counter the shortcomings of traditional EHR issues and to efficiently and effectively help in managing the Covid-19 pandemic issue by providing reliable, accurate and secure data storage and exchanges.

Literature 9:

"Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & security*, *97*, 101966. https://doi.org/10.1016/j.cose.2020.101966"

The study was undertaken by Muhammad Khurram Khan, Shuyun Shi, Debiao He, Li Li, Neeraj Kumar and Kim-Kwang Raymond Choo. The objective of the study was to understand security and privacy solutions by blockchain in EHR. It was found in the study that blockchain can be divided into three types based on permissions given to network nodes- public, private and consortium. Accuracy/integrity, security, privacy and accountability of data are some of the requirements which should be met while implementing next generation technology to secure EHR systems. Decentralization, security, immutability, autonomy and auditability are some of the properties which can be achieved using blockchain. The study concluded that blockchain has significant promise in changing the traditional healthcare business. When attempting to completely integrate blockchain technology with existing EHR systems, however a number of research and operational obstacles remain.

Literature 10:

"Anton Hasselgren, Katina Kralevska, Danilo Gligoroski, Sindre A. Pedersen, Arild Faxvaag, Blockchain in healthcare and health sciences—A scoping review, International Journal of Medical Informatics, Volume 134, 2020, 104040, ISSN 1386-5056, https://doi.org/10.1016/j.ijmedinf.2019.104040."

The study was conducted by AntonHasselgren, KatinaKralevska, DaniloGligoroski, Sindre A.Pedersen and ArildFaxvaag. The use of blockchain to improve healthcare procedures and services was outlined in a scoping review. The paper also discussed the structure of blockchain and its key characteristics. Blockchain or an immutable ledger is a decentralized log of data. Data in these blocks are bundled together, forming a chain.

Blockchian can be divided into 3 types: public, consortium and private. Smart contracts, which are self-executing contractual agreements with pre-agreed provisions written in source code, are also described by the authors.

Literature 11:

"Hylock, R. H., & Zeng, X. (2019). A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. Journal of medical Internet research, 21(8), e13592. https://doi.org/10.2196/13592"

The study was undertaken by Ray Hales Hylock and Xiaoming Zeng. They described the structure of framework.of Blockchain consists of blocks joined together forming a chain. A hash, which is similar to a unique and verified fingerprint, is used to identify each block. Each block also contains block data and the hash of the preceding block; the latter forms an unbreakable connection. When assessing the authenticity and timeliness of blocks under consideration, the blockchain uses a consensus algorithm. On reaching consensus, smart contracts are executed, thus, making sure that only with valid and legitimate data is stored.

Literature 12:

"Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Computational and structural biotechnology journal, 16, 224–230. https://doi.org/10.1016/j.csbj.2018.06.003"

The study was conducted by William J.Gordon and Christian Catalini. The article focussed on patient driven interoperability. Operational efficiency, reduced time spent on administrative tasks, reduced duplicate clinical interventions, decreased overall health system cost, decreased waste, and improved patient safety by reducing exposure to radiation or invasive procedures were all discussed as benefits of interoperability. Patient consent, governance, security, and privacy are all issues that arise as a result of the transition toward patient-centered interoperability. Blockchain is an appealing approach of solving these issues by establishing a platform for the safe exchange of data. Data aggregation, data availability, digital access rule management and immutability are some of the ways blockchian can facilitate these transactions.

FINDINGS

1. According to an article by K.T Win, over 66 percent of clients were concerned about the privacy of their personal health records, and just 39 percent of respondents believed their health information was safe and secure.

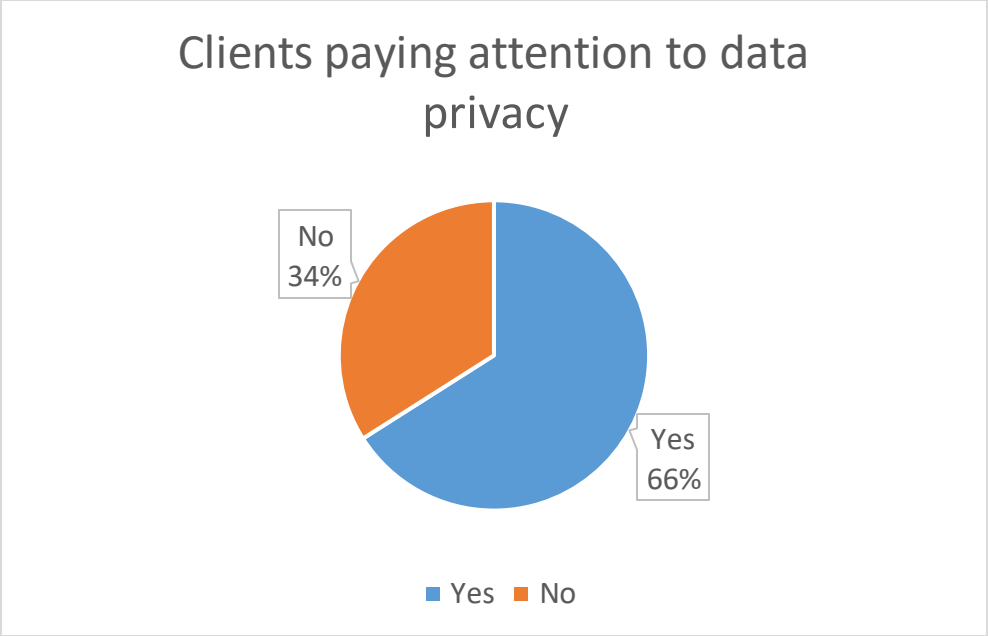

Figure 2: Source: "Security and privacy of electronic health records: Concerns and challenges, Science direct, 2020"

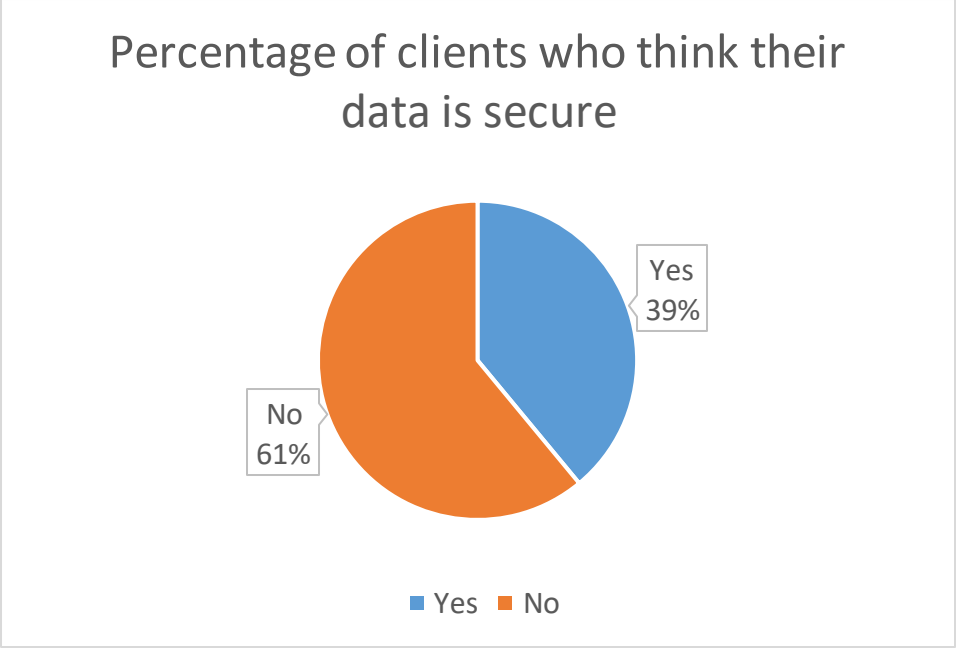

Figure 3: Source: "Security and privacy of electronic health records: Concerns and challenges, Science direct, 2020"

2. According to a study of healthcare stakeholders, 16 percent expect to utilise a blockchain-based solution in the near future, with 56 percent planning to do so by 2020.

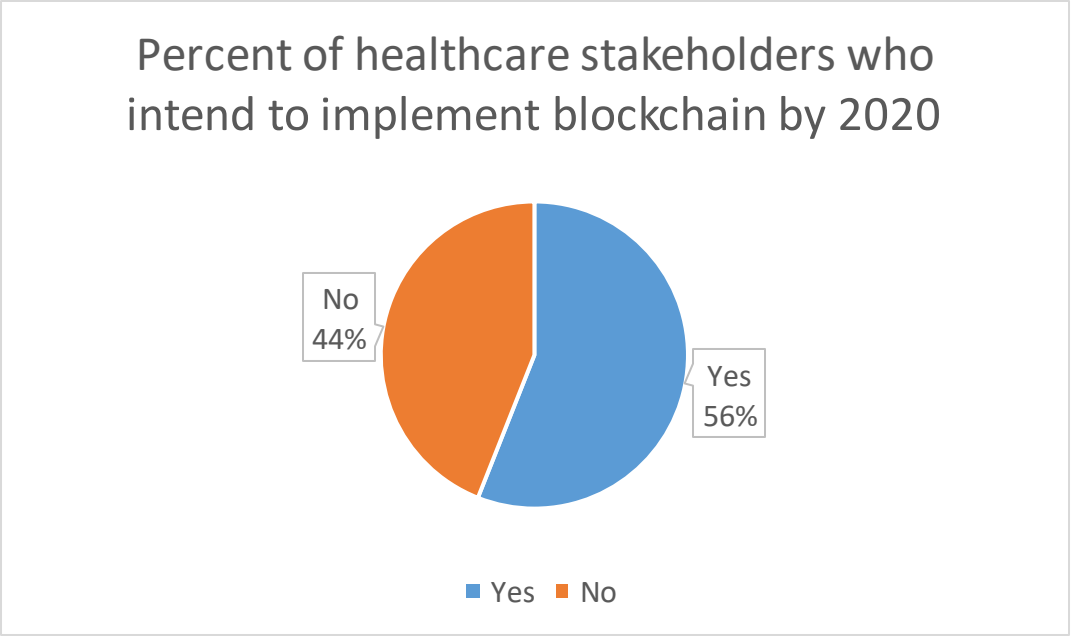

Figure 4: Source: "A Blockchain-based Framework for Securing Electronic Health Records, Research gate, 2019"

3. Smart contracts will ensure that only authorized healthcare providers can access these EHRs. The individuals/patients will be the owners of their medical data. The hospitals or research institutes will require encrypted key to get an access to the patient data. The patient will have the provision to select who can access his information and for what duration.

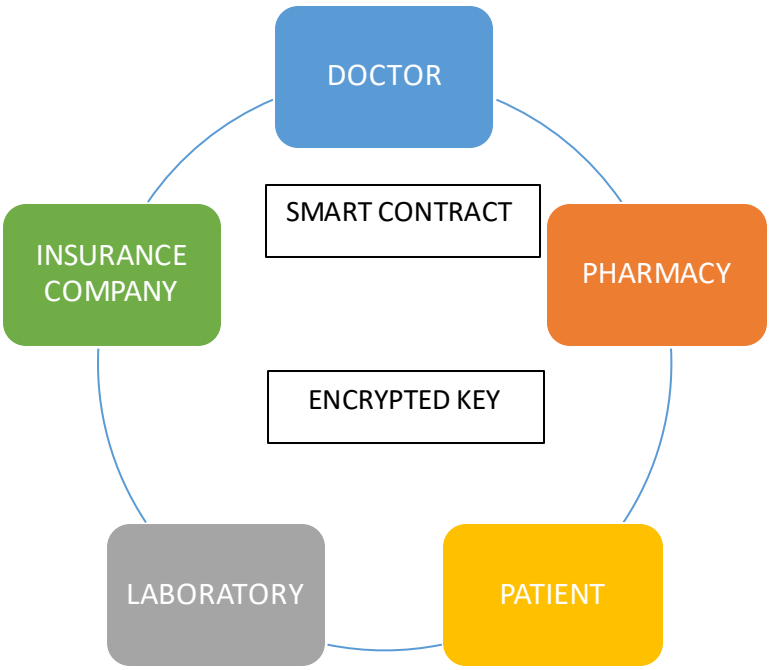

Figure 5: Source: "Towards a Blockchain Assisted Patient Owned System for Electronic Health Records, Research gate, 2021"

4. As per the global blockchain report by markets and The worldwide blockchain industry is anticipated to expand from $ 3.0 billion in 2020 to $ 39.7 billion by 2025, with a 67.3 percent compound annual growth rate (CAGR) from 2020 to 2025. The entire blockchain market will be driven by the growing desire to streamline corporate operations and the need for supply chain management solutions that are linked with blockchain technology. Emerging areas like APAC and MEA offer a plethora of untapped and undiscovered blockchain prospects.

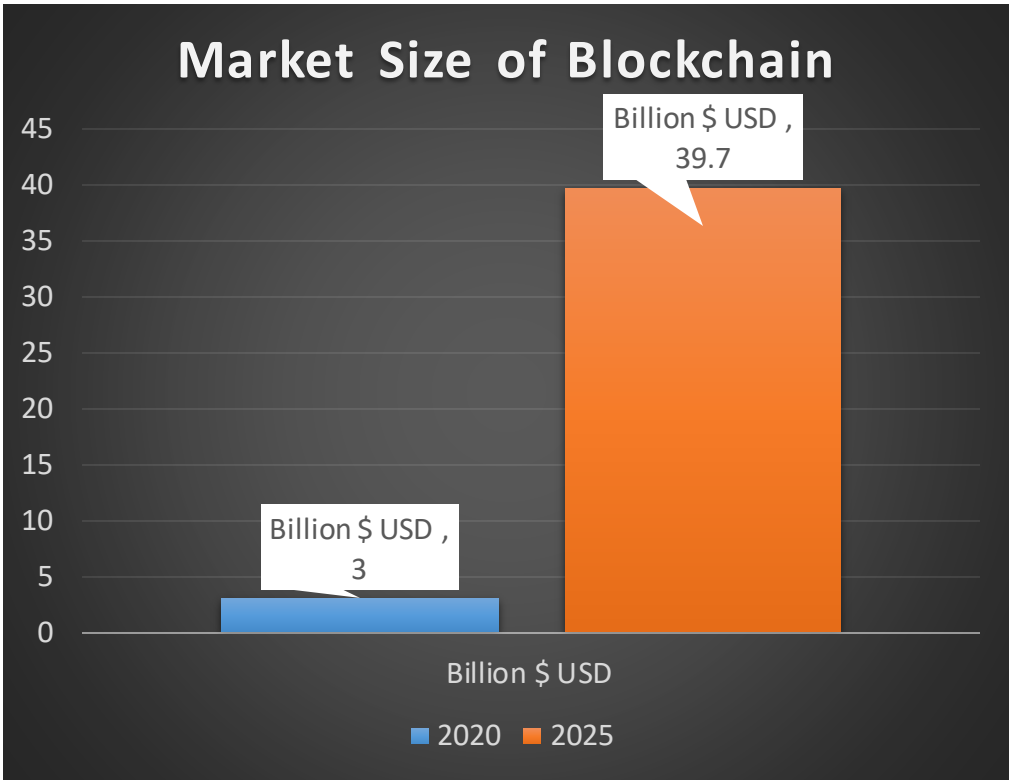

Figure 6: Source: Markets and markets Insights, 2020

DISCUSSIONS

How does blockchain work?

The blockchain technology has grown in popularity. Many industry experts believe it will be a game changer, and it has even been dubbed the "internet of value. The creation of blockchain technology may be likened to the world-changing inventions of the wheel, engine, and internet. It is even predicted to rule the next decade. All of us are familiar with Bitcoin and some of us might even confuse bitcoin as equivalent to blockchain. But the truth is, blockchain is a technology that powers bitcoin and has many more applications than bitcoin.

Decentralization is one of the most critical components of blockchain. It uses peer to peer network and eliminates the need to rely on any centralized third party or middlemen to store your data. When you transfer a sum of money to anyone, you have to rely on a bank to perform this task. But with blockchain, you can do these

transactions without the involvement of any third party. Ledger as the name suggests is the record of all transactions. Distributed ledger means that the ledger is shared with every person on the same blockchian network. Each person gets a copy of the ledger which gets updated when a new block is added on the blockchian. Once the data has been recorded inside a blockchian it becomes nearly impossible to change it, thus making it tamper proof and immutable. A new block is created after every transaction that contains all the relevant information of this transaction. The block is then sent to each node which verifies the block. Once the verification is done the block gets added to the blockchain. The verification and validation of blocks by these participating nodes is called consensus. If a specific node tampers with the block, other nodes will reject it thus making it tamper proof in nature.

As the name indicates, blockchain metaphorically consists of blocks linked together chronologically to comprise a chain known as blockchian. Every transaction or data is stored in the block. The transaction information is stored in block of the blockchian.

The first block in the blockchain is called the genesis block- it is the block from where the chain originates. Each block has 3 elements- 1) Data and transaction 2) Hash 3) Hash of the previous block. All the information related to the transaction and other information like timestamp, sender information, receiver information etc. is stored in the first element. The data contained in each block depends on the type of blockchain. For example food supply blockchian will have information of all the processes involved in that specific food supply chain. Each block also includes a Hash-a unique identifier for the block and all of its contents. Hash can be assumed as equivalent to a fingerprint. It is always unique and no two blocks can have the same hash just like the same way for fingerprints. As soon as a block is created, the hash of the blockchain gets generated simultaneously. Tampering with a block changes its hash. If hash of the block changes it indicates that the block has been tampered with and is no longer the same block. Hash can be a very powerful tool to detect any changes made in the block. Another important element that every block contains is the hash of the previous block. This piece of information is what links one block to another and makes the whole network safe and secure. In the given figure block 4 contains has of block 3 and block 3 contains hash of block 2 and so on. As discussed earlier, any change in the data of a block leads to a change in its hash. If we change the data of block 2, the hash of block 2 gets changed as well which will make the whole blockchain unstable. This happens because each block

contains hash of the previous block. When the second block is tampered the old hash becomes invalid and a new hash is generated for the block. This affects all the subsequent blocks in the chain and thus making all of them invalid. This unique property of the blockchain makes it transparent and secure because in any case of data tampering the whole network gets to know which block got compromised in the blockchain.

STRUCTURE OF BLOCKCHAIN

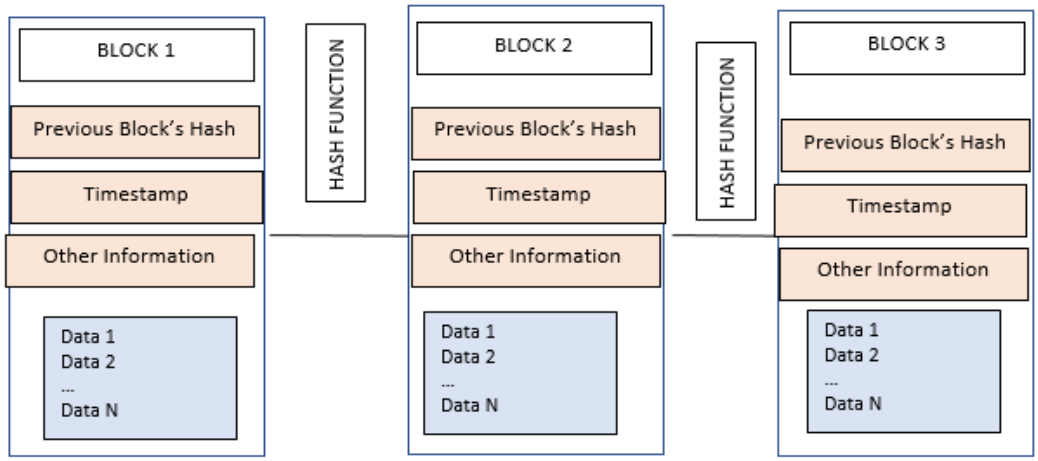

Figure 7: Source: JMIR Publications, 2019

Smart contracts are a relatively new feature to the blockchain technology. Smart contracts function in the same way as real-world contracts do. Smart contracts, on the other hand, are entirely digital and are kept on the blockchain. Smart contracts, unlike traditional contracts, are made up of software code that is performed by the blockchain network. The beauty of smart contracts is that they can't be changed once they've been decided. This section holds rules for negotiating contract terms, automatically validates the contract, and then executes the terms that have been agreed upon. Contract execution and implementation do not need any manual involvement. The use of blockchain in conjunction with smart contracts eliminates the need for third parties. By delivering a contract-invoking transaction to the necessary contract address such a system can achieve sophisticated programmed tasks. Then, smart contract will execute the predefined terms in the secure container automatically. When the parameters meet

the defined conditions in the smart contracts, action is executed as per the condition mentioned in the smart contract.

What is the application of blockchain in EHR?

A medical record used to be simply information put down for scientific, therapeutic, administrative, and economical purposes. It had a severe limitation in terms of accessibility, and it could only be used by one person at a time. It took anything from 1 to 6 months or more to finish because it was updated manually. Many of the problems connected with wrong prescriptions, doses, and procedures are eliminated when records are legible. Furthermore, when EHRs are linked to drug banks and pharmacies, adverse medication responses can be significantly avoided. This can be achieved by restricting the prescription and ordering of medications for which a known adverse reaction in a specific patient has been documented. Accessibility from anyplace at any time is also advantageous. They take up less room in storage and may be kept permanently. They help researchers, reduce the number of records lost, offer a comprehensive set of backup records at a cheap cost, speed up data transfer, and are cost-effective. Hence, EHR helps in providing accessibility of data and better care for the patients.

Today EHR of an individual are in an unstructured manner and controlled by health care providers in their respective central databases. These databases lack interoperability, security and are very vulnerable to hacking. Despite the fact that computers are in virtually every medical institution and mobile phones are in nearly everyone's pockets. We're still having trouble gathering, exchanging, and sharing our medical records with a new doctor. Sharing medical data between various healthcare providers, while maintaining privacy and integrity of the patient's data is the biggest challenge that healthcare systems face today. The healthcare system is not digitized everywhere in the world. Many healthcare providers still follow the traditional process and provide prescriptions on paper and graphs. In such scenario, it becomes difficult for both patients and healthcare providers to refer to these prescriptions whenever required in the future. The healthcare system works in silos and lack interoperability. Even the healthcare systems of different departments within the same hospital are unable to interact with each other. It becomes challenging for the patient to procure his clinical history and share that with the new service provider. All diagnostic test have to be performed again to know the exact problem, thus resulting in a delayed treatment and further aggravation of the issue. When the doctor is treating a patient who needs

emergency care, it becomes difficult for him to know if the patient is allergic to any specific medicine. The doctor needs to be extra cautious and has to perform the drug allergy tests to validate this because the consequences can be quite dire if the patient is administered any such medicine that he is allergic to. It is nearly impossible for hospital pharmacies to have a clear picture of the patient data. This in turn becomes a challenge for them to predict the inventory required to meet the needs of the hospitals. Every time a patient consults online he is required to fill all his history details. There is no effective way for patients to share their health data with the healthcare provider effectively through the remote technology.

Privacy

Privacy defined by Justices Samuel Dennis Warren and Louis Brandeis as the right "to be left alone." As described by Richard Rognehaugh, the right of an individual to avoid personal information from being disclosed to others; the claim of people to be free of surveillance or intrusion by other individuals, organisations, or the government. Only with the patient's agreement or as required by law may information about a patient be shared with others. When a patient is unable to do so because of age or mental incompetence, the patient's legal representative or legal guardian should make decisions about information sharing on his or her behalf. Many surveys have revealed a high level of worry about the privacy of health information. It was found in an article by Ismail Keshta and Ammar Odeh that nearly 66% of clients were concerned about the privacy of their personal health records, with just 39% believing that their information was secure and safe. Many people feel that disclosing their health information would jeopardise their privacy. Patient's intention of sharing their health information online is impacted negatively by rising concerns on the privacy of their medical data. Patients also have sensitive personal information related to infertility issues, abortion, sexually transmitted diseases among other issues that would have an impact on their mental health as well if it is accessed by other stakeholders in EHR. Health care organisations, insurance companies, and others will require access to the data if EHRs are to function properly. Limiting access to information to just those who are authorised is crucial to protecting privacy. The first step is to give people permission to use the system.

Every patient will have a unique identity on the blockchain network, and his clinical data will be linked to this identity as an EHR digital asset at various phases. While blockchain technology will help the individuals to maintain their EHRs. Combining

blockchain technology with an access control mechanism looks to be a feasible option for building a secure system. Patients may predefine access rights (authorise, deny, revoke), operations (read, write, update, delete), and duration to share their data using smart contracts on the blockchain without losing control. When all of the preconditions are satisfied, smart contracts would be activated on the blockchain and it will offer an audit mechanism for every request recorded in the ledger. Smart contracts would ensure that only authorized healthcare providers can access these EHRs. The individuals/patients will be the owner of their medical data. The hospitals and research institutes will require encrypted keys to get an access to the patient data. The patient will have the provision to select who can access his information and for what duration. Individuals can also preauthorize the healthcare providers to see their information during any unforeseen emergencies.

Interoperability

The potential to share the information is referred to as interoperability. To be genuinely interoperable, two EHR systems must be able to share and then use data. A large number of government-certified EHR solutions, each with its own technical requirements, functional capabilities, and clinical terminology are in use across each nation. It's challenging to create a common interoperability format for transferring data because of these variances. Sometimes because EHR systems are frequently heavily tailored to an organization's particular workflow and preferences, they are not compatible when developed on the same platform. When two EHR systems are able to share information and use data, they are considered to be interoperable.

Every patient will have a unique identity on the blockchain network, and his clinical data will be linked to this identity as an EHR digital asset at various phases. Blockchain can provide a truly interoperable network. Whenever a patient will undergo any diagnostic test or consultation, this information will be incorporated into patient's unique electronic health chain. Even the health related data collected from smart devices can also be securely incorporated into it. This EHR data can then be easily exchanged among various health providers as and when needed. This would even reduce the cost of healthcare treatment by avoiding the redundant diagnostic test. The healthcare provider can give better patient care on the basis of this accurate data.

Data security & Immutability

Security breaches occur when sensitive health information is made available to other parties without the individual's consent or authority. The major sources of security concerns were inappropriate employee usage or insider employee misbehaviour as well as physical theft of data storage equipment like hardware and computers in the early years of EHRs. The potential threat categories can be categorized as – administrative, technical, physical, insider use and portable devices. Newer security issues and techniques of obtaining sensitive health information have emerged as cyber thieve's skill has risen in recent years. Healthcare businesses are no strangers to threats and breaches. The healthcare business like other industries, has not kept up with the growing cyber risks that digitalization has brought to their enterprises. In addition, healthcare businesses do not invest as much in cyber-security as their counterparts in other industries, such as banking or retail. Due to a lack of follow-up, cyber-attacks have become more targeted and vulnerable. Two events of security breaches took place in the year 2013 at Howard University Hospital where patients' names, addresses, social security numbers, diagnosis related information and Medicare numbers for more than 34,000 patients were compromised. 68% of the healthcare organizations that were surveyed in US reported that they had recently experienced a significant security incident which comprised of security incidents from insider and external threats. An article by Khin Than Win discussed several security breach events- (1) patient records being exposed on the internet (2) patient name of 4000 HIV positive patients sent to Florida newspapers (3) A hacker gained access to the University of Washington Medical Center's computer system and stole information of 5000 cardiology and rehabilitation medicine patients. (4) The identities of dead kidney donors were accidentally released by the University of Minnesota.

Blockchain is now one of the most secure data security solutions available. Rapid developments in digital technology have resulted in new data security issues. A distributed ledger system's high level of security is advantageous for building a secure data network. Businesses that provide consumer products and services use blockchain technology to keep track of customer information. Blockchain technology is capable of handling everything and ensuring that data is not tampered with in any manner. Because it is encrypted by nature, it is possible to do adequate validation. The information can

only be decrypted with the aid of a key given by the person who is providing the information. As the name suggests blockchain is a chain of digital blocks which contain different information. Since, it is not stored in a central location, the data cannot be tampered from a single computer. Each block is connected with blocks after and before it. Usually hackers hack the information from the central point of contact where all the information is present but blockchain makes it hard for hackers thus providing security to the data.

Once the data has been recorded inside a blockchian it becomes nearly impossible to change it, thus making it tamper proof and immutable. A new block is created after every transaction that contains all the relevant information of this transaction. The block is then sent to each node which verifies the block. Once the verification is done the block gets added to the blockchain. The verification and validation of blocks by these participating nodes is called consensus. If a specific node tampers with the block, other nodes will reject it thus making it tamper proof in nature.

Challenges in EHR	**Benefits of blockchain technology**
Privacy	Eliminates third party involvement. Smart contracts ensures that the data can only be used or viewed by anyone if certain conditions have been specified in the smart contract. Hospitals and research organizations require encrypted keys to access patient data.
Interoperability	EHR data can then be easily exchanged among various health providers as and when needed. Data can be accessed by different departments of the hospital. Oxygen saturation level, BPM, BP, daily step count, calorie intake etc. can be integrated with patients EHR, so that doctor can provide better consultation. Interoperable EHR data reduces the chances of prescription of wrong drug to patient. It would also reduce the overhead

	cost for hospitals and healthcare providers.
Data security & Immutability	Encryption key and distribution ledger technology ensures data to be more secure as compared to EHR security. Previous and next blocks are connected to each other. If any change is made on any of block it would result in changing the hash number. Therefore making it immutable.

CONCLUSION

Although EMRs have several advantages, the future of health care necessitates that their dangers be identified and effectively handled or avoided. Privacy, interoperability, data security and immutability are some of the challenges which can be solved with the help of blockchain. Blockchain when combined with encrypted keys and smart contracts ensure privacy and security to patient's data. Blockchain works through distributed ledger technology therefore possessing the properties of – decentralized, distributed ledger and immutability. Once implemented the electronic health records on blockchain will serve as a common and integrated backbone for the health industry.

RECOMMENDATIONS

The COVID 19 pandemic has also reiterated the importance of businesses have to be future-ready to enable a transformative customer experience. In fact, the impact of Covid has made people realize that insurance is no more a priority but a necessity Furthermore, today's customers are well-connected, respond swiftly, and are not hesitant to accept new technology that may immediately improve their lives.

Blockchain technology in EHRs will be the next step to empower end customers. The consumers will be able to see their transactions and can grant permission if their insurance agent, physician or pharmacist want to look at their records. Also, blockchain has would ensre transparency and operational efficiency and prevent cyber-hacking of information.

Team members and decision makers should be trained beforehand about the disruptive potential of blockchain adoption in EHRs along with making necessary infrastructure investment.

While integrating such technology may appear to be time-consuming and costly, it is ultimately in the best interests of public health. With the broad adoption of blockchain technology, the actual value in industry is expected to emerge from collaborating on a single platform to give true interoperability capabilities that did not previously exist. EHRs are undergoing a revolution as a result of the introduction of blockchain technology.

REFERENCES

Ozair, F. F., Jamshed, N., Sharma, A., & Aggarwal, P. (2015). Ethical issues in electronic health records: A general overview. *Perspectives in clinical research*, *6*(2), 73–76. https://doi.org/10.4103/2229-3485.15399

Ismail Keshta, Ammar Odeh, Security and privacy of electronic health records: Concerns and challenges, Egyptian Informatics Journal, Volume 22, Issue 2, 2021, Pages 177-183, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2020.07.003.

Ayanthi Jayawardena, A systematic literature review of Security, Privacy and Confidentiality of patient information in Electronic Health Information Systems, Sri Lanka Journal of Bio-Medical Informatics,2021, DOI: 10.4038/sljbmi.v4i2.5740.

McDermott, D.S., Kamerer, J.L., & Birk, A.T. (2019). Electronic Health Records: A Literature Review of Cyber Threats and Security Measures.

Khin Than Win, A Review of Security of Electronic Health Records, The HIM journal 34(1):13-8,2005, DOI: 10.1177/183335830503400105.

Reisman M. (2017). EHRs: The Challenge of Making Electronic Data Usable and Interoperable. *P & T : a peer-reviewed journal for formulary management*, *42*(9), 572–575.

J. Vora et al., "BHEEM: A Blockchain-Based Framework for Securing Electronic Health Records," 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1-6, doi: 10.1109/GLOCOMW.2018.8644088.

Alam, S.; Ahmad Reegu, F.; Daud, S.M.; Shuaib, M. Blockchain-Based Electronic Health Record System for Efficient Covid-19 Pandemic Management. Preprints 2021, 2021040771 doi: 10.20944/preprints202104.0771.v1

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & security*, *97*, 101966. https://doi.org/10.1016/j.cose.2020.101966

Anton Hasselgren, Katina Kralevska, Danilo Gligoroski, Sindre A. Pedersen, Arild Faxvaag, Blockchain in healthcare and health sciences—A scoping review, International Journal of Medical Informatics, Volume 134, 2020, 104040, ISSN 1386-5056, https://doi.org/10.1016/j.ijmedinf.2019.104040.

Hylock, R. H., & Zeng, X. (2019). A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study. Journal of medical Internet research, 21(8), e13592. https://doi.org/10.2196/13592

Gordon, W. J., & Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Computational and structural biotechnology journal, 16, 224–230. https://doi.org/10.1016/j.csbj.2018.06.003

Towards Data Science. Blockchain Technology Ensuring Data Security & Immutability; 2020

https://towardsdatascience.com/blockchain-technology-ensuring-data-security-immutability-7150d309352c

Markets and markets. Blockchain Market by Component, Provider, Type, Organization Size, Application Area, and Region - Global Forecast to 2025; 2020

https://www.marketsandmarkets.com/Market-Reports/blockchain-technology-market-90100890.html