BLOCKCHAIN BASED SOLUTION FOR ELECTRONIC HEALTH RECORDS: A REVIEW

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

Dr. MALVIKA SHEKHRI

Under the Supervision and Guidance of

Dr. SEEMA MEHTA

2022

BLOCKCHAIN BASED SOLUTION FOR ELECTRONIC HEALTH RECORDS: A REVIEW

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

Dr. Malvika Shekhri

Under the Supervision and Guidance of

Dr. Seema Mehta

2022

DECLARATION BY STUDENT

I hereby declare that this dissertation titled Blockchain based solution for Electronic Health Records: A Review 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 Information derived from the published or unpublished work of others has been duly acknowledged in the text.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 – Dr. Malvika Shekhri

Date- 1-7-22

m16
LABS

Internship Completion Letter

Internship Completion Letter

Date : Mar 22, 2022 to 19th July, 2022

Subject : Completion of Internship Letter

To Whomsoever It May Concern,

M16labs certifies that Dr. Malvika Shekri successfully completed the internship program at our organization as a Business Development Intern.

During this time, Dr. Malvika worked on the development of key health Information Technology related business development projects.

By working on these projects, Dr. Malvika acquired critical Professional skills.

Dr. Malvika displayed professional traits during her internship period and managed to complete all assigned tasks as requested. She was hardworking, dedicated, and committed. It was a pleasure having her with us in this period.

Yours [illegible],

Anil Li

Founder & CEO

Meta16labs Healthcare & Analytics Private Limited

CERTIFICATE

This is to certify that dissertation titled is a record of the research Blockchain based solution for Electronic Health Records: A Review work undertaken by Dr Malvika Shekhri 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.

Dr. Seema Mehta
Faculty Guide
IIHMR University, Jaipur

Date: 1st July 2022

Dhirender Kumar
School Dean
IIHMR University, Jaipur

Date- 1st July 2022

ABSTRACT

1. **Background:**

In today's smart cities and homes, patients' private information, including names, addresses, and diseases, is frequently compromised, which is inextricably linked to the security of the electronic health records, (EHRs). The majority of the time, patients cannot access data because of the most advanced security procedures in place for EHRs. These schemes struggle to strike an effective balance between data privacy, data security, interoperability, and the requirement for patients and clinicians to engage with data on a regular basis. Blockchain technology solves the problems listed above by sharing data in a decentralized and transactional manner. This can be utilized in the healthcare sector to find a balance between accessibility and EHR privacy, storage efficiency, privacy, and security. This dissertation project will explore Block chain-based framework for efficient data storage, privacy, and security for the management of EHRs in this study. The purpose is to look at how blockchain works and how it might assist EHRs become more secure.

2. **Objectives:**

- To know the technology of Blockchain and how does it work.
- To know the position of the Blockchain in healthcare market.
- To investigate the application of Blockchain to strengthen Electronic Health Record.

3. **Methodology:** The secondary research data provide the foundation of the paper. Data was gathered from previous publications about blockchain and its use in electronic health records after reading them. To comprehend the structure of blockchain, articles relevant to it were also reviewed.

4. **Keywords:** Blockchain, EHR, Security, Privacy, Interoperability, Smart Contracts

ACKNOWLEDGEMENT

The process of learning never ends. We eventually succeed because of our constant desire to learn more by seizing any chance that comes our way.

I want to express my gratitude to the management for giving me this chance to learn more about blockchain-based solutions for enhancing electronic health records. In order to get the most value out of all the material at my disposal and turn this chance into a lovely learning experience, I was able to explore the subject from every angle while working on this report.

I would want to express my deep gratitude to my mentor, Dr. Seema Mehta, who has helped me immensely and pointed me in the right direction throughout my learning experience.

I also want to express my sincere gratitude and appreciation to Mr. Anil JJ the organisation manager, and Mr. Arnav Mahurkar, the organisation mentor, for their consistent encouragement and helpful suggestions that helped me finish my project report.

Finally, I acknowledge my inability to verbally express my gratitude to my beloved family for their unwavering belief in me and for their ongoing support and encouragement.

Above all, I give thanks to God for providing me the endurance and fortitude to successfully navigate the challenges that arose during this endeavor.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION- (CHAPTER-1)

1.1 Blockchain: Blockchain is a whole system for storing data in the way that makes a system change, hacking, and cheating difficult or most probably impossible. A blockchain is a very simply network of computer systems that duplicates, distributes digital ledger of transactions across the entire network present in the system. Each block, on the chain comprises a number of transactions, and each participant's ledger receives a copy of each new transaction that takes place on the blockchain. Distributed Ledger Technology refers to the decentralised database that is governed by numerous users, (DLT). Transactions on a blockchain are recorded with an immutable cryptographic signature known as a hash.

- Source: Euromoney learning

1.2 TYPES OF BLOCKCHAINS:

Public Blockchains: With public blockchains, any member has access to the blockchain's data and may take part in the consensus process, creating a totally decentralised network.

Private blockchains: Dedicated to single enterprise solutions, private blockchains are used to track data transfers between various departments or individuals. Each participant must first approve of joining the network before being recognised as a member.

Blockchain consortiums: A blockchain consortium is a permissioned network that only a select group of users can access. It is used as a distributed database that tracks participant data exchanges and is auditable and consistently synchronised.

Hybrid Blockchains: It mix the benefits of public and private blockchains. As a result, a private blockchain operates in the background to control access to the ledger's modifications while a public blockchain is utilized to make the ledger totally accessible.

-Source: Springer Link

1.3 KEY FEAUTURES OF BLOCKCHAIN:

1.3 (a) Decentralization

With blockchain, data is dispersed throughout the network rather than being centralised. Due to shared input from the network's connected nodes, this also enables the distribution and management of information under consensus. Many reputable organisations now handle the data that was once centralised at one location**.**

.3 (b) Data Transparency

In order to achieve data transparency in any system, relationships between entities must be based on trust. The relevant data or record needs to be protected and weatherproof. Any data saved on the blockchain is dispersed throughout the network and is not concentrated in one area or under the control of a single node. Since data ownership has been divided, it is now transparent and protected from outside interference.

1.3 © Security and Privacy

In order to achieve data transparency in any system, relationships between entities must be based on trust. The relevant data or record needs to be protected and weatherproof. Any data saved on the blockchain is dispersed throughout the network and is not concentrated in one area or under the control of a single node. Since data ownership has been divided, it is now transparent and protected from outside interference.

-Source: IEEE Access

1.4 **EHR: Electronic health record (EHR)** is the organised gathering of patient and population health data that has been digitally preserved. The sharing of these records is possible between various healthcare facilities. Records are exchanged via additional information networks and exchanges, including network-connected, enterprise-wide information systems. In addition to billing information, demographics, medical history, prescription and allergy information, immunisation status, laboratory test results, radiographic images, and vital signs, EHRs may also incorporate other types of data.

-Source: Health IT.gov

1.5 Advantages of using EHR for healthcare providers-

EHRs and the capacity to exchange health information electronically can improve your organization's operations and help you give patients better, safer treatment. EHRs assist providers in improving patient care management and delivery through:

- At the point of care, giving patients complete, accurate, and current information
- Facilitating quick patient record access for more coordinated, effective care
- Securely exchanging electronic data with patients and other medical professionals
- Assisting medical professionals in safer care delivery, medical error reduction, and patient diagnosis.
- The convenience of health care, engagement between patients and providers, and enabling more dependable, safer prescription
- Supporting the advancement of clear, comprehensive documentation and precise, efficient coding and invoicing
- Improving the security and privacy of patient data.

-Source: Health IT.gov

1.6 Disadvantages of using EHR:

- Cybersecurity and Privacy Concerns

EHR systems are not immune to hacker attacks, which can affect all electronic systems. Negative outcomes may occur if private medical information gets into the wrong hands.

- False Information

Everyone using an EHR could be receiving inaccurate or partial information if it is not updated right away whenever new information is available, such as following an exam or when test results are received. This could eventually result in mistakes being made by the practitioner issuing the prescription as well as any specialists, pharmacists, physical therapists, or personal trainers involved in the patient's care in terms of diagnosis, treatment, and health outcomes.

- Fear-Mongering Patients Without Need

A patient may be exposed to facts that they may not fully grasp if they have free access to their own medical records. Accessing information that one does not completely understand could lead to a number of misunderstandings, some of which could cause the patient to panic or respond in an inappropriate way that could be dangerous.

- Concerns about Malpractice Liability

Implementing an EHR system raises a number of liability issues, such as how to prevent the loss or destruction of sensitive medical data when moving paper electronic records. Errors in treatment could result from this in turn.

Having access to federal financial incentives, enhanced service quality, more convenience and efficiency, and electronic health records are just a few of the many advantageous features that both patients and providers may take advantage of. They do, however, also have a number of potential drawbacks that should be taken into account. These include some inconveniences and inefficiencies, as well as potential privacy and cybersecurity concerns, the possibility of unnecessarily terrifying patients, an increase in the risk of malpractice liability, and problems with cost in terms of both time and money. These issues can be fixed with blockchain.

-Source: Health IT.gov

1.7 RATIONALE

With the evolution of technology and rising customer demand, it's more vital than ever to consider how we can use emerging technologies like blockchain to maintain transparency and use trust to improve the value offer. The goal of the research is to learn more about blockchain and how blockchain can be used to improve the security of electronic health records.

1.8 RESEARCH QUESTION

What are some of the ways that blockchain-based technologies can be used to improve electronic health records?

1.9 OBJECTIVES:

- To know the technology of Blockchain and how does it work.
- To know the market position of the Blockchain
- To investigate the application of Blockchain to strengthen Electronic Health Record.

METHODOLOGY (CHAPTER-2)

Study design- Desk Review

Type of data- Secondary Data

Study tools- Research papers, blogs, surveys, analyst reports on relevant blockchain topics, ResearchGate, google scholar, PubMed etc. Information was searched across internet, journals, thought leadership papers, blogs, news articles and published studies in order to collect the material inclusion criteria.

Duration of study- 3 months

RESEARCH PAPER COLLECTION:

INITIAL DATA GATHERED FROM SOURCES MENTIONED BELOW	**FILTER OF DATA BASED ON INCLUSION CRITERIA**	**UTILIZED IN FINAL REPORT**
Research paper (21) **Google Scholar, pubmed**	7 research paper found in inclusion criteria	2 papers were finally used to understand and define the structure of Blockchain
Reports, Industry reports (11)	**2 Reports,** **3 Industry reports** found in inclusion criteria	Reports were used for statists, such as market size and industry data
Blogs (25)	15 **Blogs** found in inclusion criteria	Current implementation and developments were taken from blogs.
Journals (9)	**4 Journals** found in inclusion criteria	Findings were used for the conclusion part.
Articles (Newspaper, revies, opinion, surveys) **(11)**	**5 Newspaper,** **2 revies,** **0 opinion, surveys** found in inclusion criteria	News in transition and global trends, future possibilities were taken from this.

Inclusion criteria- (a) Objective 1- Articles from 2015 onwards, originating from India.

(b) Objective 2- Articles from 2012 onwards.

Exclusion criteria- (a) Objective 1- Articles before 2015 and not originating from India.

(b) Objective 2- Articles before 2012.

LITERATURE REVIEW (CHAPTER-3)

Most Literatures have emphasis on security aspect of blockchain technology and used term privacy, security, and confidentiality, The confidentiality of personal health records was a source of concern. There were some reservations about health information. (Ismail Keshta, 2021; Ammar Odeh, 2021). EHR has numerous advantages, including lowering the problem of incorrect prescriptions, doses, and procedures by providing legible data. When EHRs are linked to pharmacies and drug banks, adverse drug response incidents are decreased. (Amit Sharma, 2015; Praveen Aggarwal, 2015; Fouzia F. Ozair, 2015; Nayer Jamshed, 2015). Medical claims/billing management, medical research, patient data security, and medicine supply chain can all benefit from the adoption of blockchain. The results show that by combining specialised nodes with improvised authority, unwanted access by various actors is further minimised and sense of decentralisation is established. 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. (Sudhanshu Tyagi, 2018; Jayneel Vora, 2018; Sudeep Tanwar, 2018; Anand Nayyar, 2018; Joel Rodrigues, 2018; Neeraj Kumar, 2018). Patients refusing to provide their personal information to health care providers, providing incorrect patient personal information to medical institutions, and requesting the removal of patient personal information are all examples of violations of patient privacy. Because if sensitive information is leaked to a third party, the patient may face serious consequences, EHR security and privacy issues are crucial. (Ismail Keshta, 2021; Ammar Odeh, 2021). Gain additional knowledge about the suggested blockchain-based approach for EHR data transfer, storage, privacy, and security. healthcare stakeholders found that 16 percent anticipate

using a blockchain-based solution soon, and 56 percent intend to do so by 2020. (Sudhanshu Tyagi, 2018; Jayneel Vora, 2018; Sudeep Tanwar, 2018; Anand Nayyar, 2018; Joel Rodrigues , 2018; Neeraj Kumar, 2018)

The majority of patients were concerned about the privacy and security of their electronic health records, however many believed that the benefits outweighed the dangers. The primary challenges with EHRs were identified as security, privacy, and confidentiality. Because none of them were completely secure, and just two of them (eight percent) were HIPAA-compliant. (Ayanthi, 2021; Jayawardena, 2021). EHR takes up less storage space and can be kept for an indefinite amount of time. EHRs aid research, provide, a complete, set of backup records at a minimal cost, speed up data transfer, and are cost-effective. (Amit Sharma, 2015; Praveen Aggarwal, 2015; Fouzia F. Ozair, 2015; Nayer Jamshed, 2015). Unauthorized access to EHRs, unauthorised exposure of sensitive data, potential data fraud, and data manipulation were all mentioned in the study as major privacy and security risks. (Ayanthi, 2021; Jayawardena, 2021). Despite the government's efforts to protect EHR, it is being targeted by cyber criminals. In 2015, there were 187 documented data breaches involving 84 million patients' personal information. Healthcare breaches accounted for 21% of all cyber security breaches worldwide. (Donna S. McDermot, 2019; Jessica L. Kamerer, 2019; Andrew T. Birk, 2019). Loss and destruction of data also occurs during data transfer which leads to inaccurate information being sent to insurance companies. (Amit Sharma, 2015; Praveen Aggarwal, 2015; Fouzia F. Ozair, 2015; Nayer Jamshed, 2015). Administrative, technological, physical, insider use, and portable devices were all listed as potential threats. (Donna S. McDermot, 2019; Jessica L. Kamerer, 2019; Andrew T. Birk, 2019).

Blockchain technology can be used to achieve a number of qualities, including decentralisation, security, immutability, autonomy, and auditability. According to the study's findings, blockchain holds great promise for revolutionising the conventional healthcare industry. (Muhammad Khurram Khan, 2020; Shuyun Shi, 2020; Debiao He, 2020; Li Li, 2020; Neeraj Kumar, 2020; ; Kim-Kwang Raymond Choo, 2020).There are still a ,number of operational, research challenges when, attempting to ,fully ,integrate ,blockchain ,technology with current ,EHR systems. (Muhammad Khurram Khan, 2020; Shuyun Shi, 2020; Debiao He, 2020; Li Li, 2020; Neeraj Kumar, 2020; ; Kim-Kwang Raymond Choo, 2020). Some needs that should be satisfied while

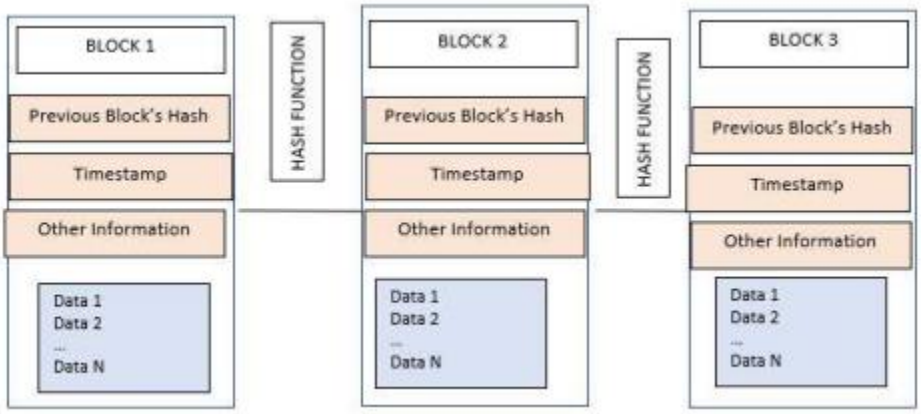
installing next-generation technology to safeguard EHR systems include accuracy/integrity, security, privacy, and accountability of data. (Muhammad Khurram Khan, 2020; Shuyun Shi, 2020; Debiao He, 2020; Li Li, 2020; Neeraj Kumar, 2020; ; Kim-Kwang Raymond Choo, 2020). By providing a secure method for transmitting medical data by safeguarding it through peer-to-peer connection, blockchain can be utilised to improve and modernise electronic health record exchanges. Better patient information access, interoperability, security, privacy, and immutability are all benefits of blockchain technology. (Shabad Alam, 2021; Mohammed Shuaib, 2021**)**

RESULTS AND DISCUSSIONS (CHAPTER-4)

The blockchain technology has become increasingly popular. Many experts believe it will be a game changer, and it has even been termed the "internet of value" by others. The invention of blockchain technology is comparable to the wheel, engine, and internet, all of which changed the world. It's even expected to control the next ten years. We've all heard of Bitcoin, and some of us may even consider it to be the same thing as blockchain. However, blockchain is a technology that underpins bitcoin and has far more uses than bitcoin. One of the important part of blockchain - decentralisation. It uses a peer-to-peer network to store data, eliminating the need for any centralised third parties or middlemen. When you need to send a large sum of money to someone, you must entrust the work to a bank. However, with blockchain, these transactions can be completed without the intervention of a third party. As the name implies, a ledger is a record of all transactions. The term "distributed ledger" refers to a ledger that is shared by everyone on the same blockchain network. When very new block added to the blockchain, each person receives a copy of the ledger, which is updated. It is nearly impossible to modify data after it has been recorded inside a blockchain, making it tamper-proof and immutable. After each transaction, a new block is created that contains all of the transaction's relevant data. After that, the block is forwarded to each node, which verifies it. The block is added to the blockchain once the verification is completed. Consensus is the process of these participating nodes verifying and validating blocks. Other nodes will reject the block if one node tampers with it, making it meddle proof in nature.

As the name implies, blockchain is a metaphor for a chain of blocks linked together chronologically to form a blockchain chain. The block stores all transactions and data. The transaction data is saved in the blockchain's block.

4.1 STRUCTURE OF BLOCKCHAIN



Figuree 1: Source: JMIR Publications, 2019

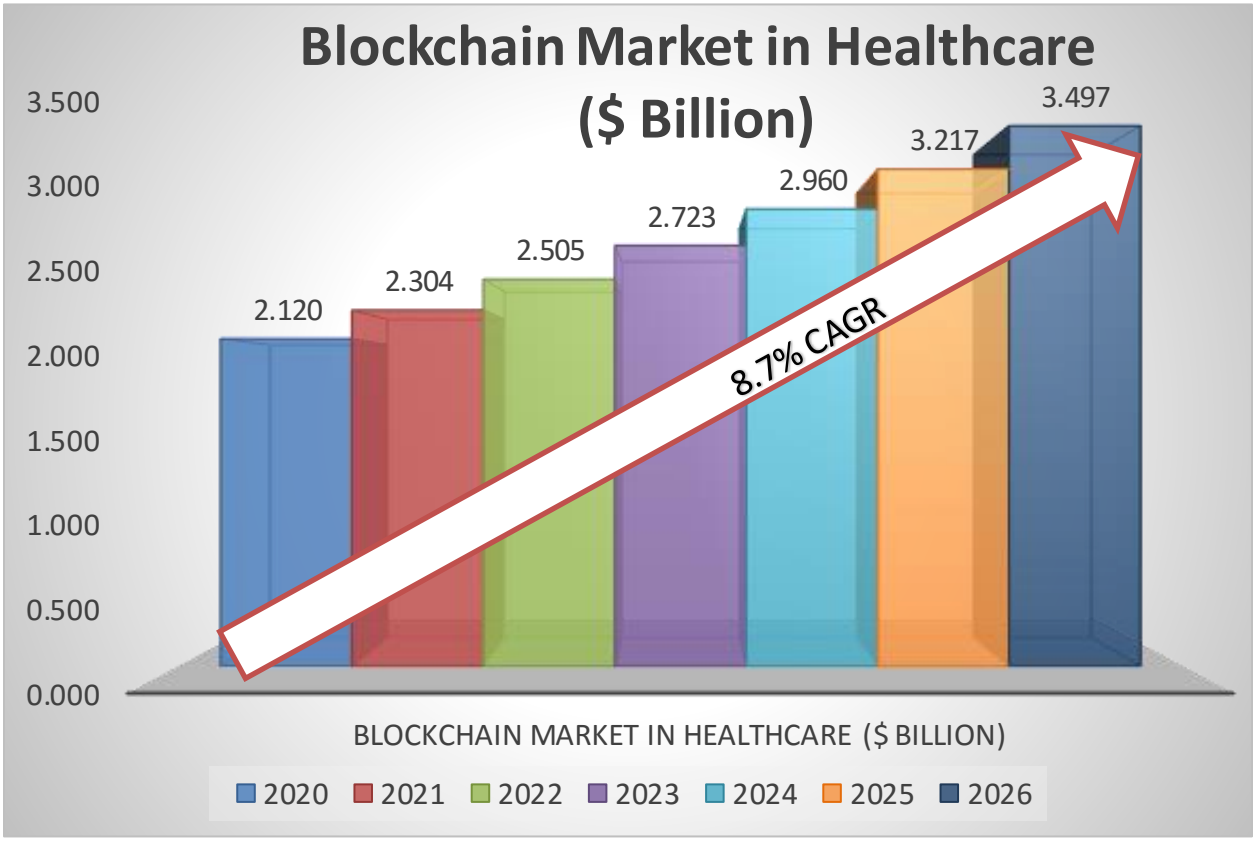
The genesis block is the first block on the blockchain, and it is the block from which the chain is formed. Each block consists of three elements: 1) data and transaction; 2) data and transaction; and 3) data and transaction. 2) The hash 3) The previous block's hash. The first element stores all transaction-related information as well as other data such as timestamps, sender information, recipient information, and so on. The data stored in each block varies depending on the blockchain type. Food supply blockchain, for example, will have data on all of the operations involved in that specific food supply chain. Each block also has a Hash, which serves as a unique identifier for the block and its contents. A fingerprint can be presumed to be equivalent to a hash. It is always unique, and no two blocks can have the same hash, just as fingerprints cannot have the same hash. When a block is created, the blockchain's hash is generated at the same time. The hash of a block is changed when it is tampered with. If the block's hash changes, it means the block has been tampered with and is no longer the same block. Hash can be a very effective method for detecting changes in a block. Every block also contains the hash of the previous block, which is a significant feature. This data is what connects one block to the next and keeps the entire network safe and

secure. Block 4 includes the hash of block 3, and block 3 contains the hash of block 2, and so on. As previously stated, any change in a block's data results in a change in its hash. If the data of block 2 is modified, the hash of block 2 is also changed, making the entire blockchain insecure. Because, each block contains hash of recent block, this occurs. When the second block is tampered with, the previous hash for the block becomes invalid, and a new hash is created. This has an effect on all subsequent blocks in the chain, rendering them all invalid. This one-of-a-kind quality of the blockchain makes it transparent and secure, because in the event of data tampering, the entire network will know which block in the blockchain has been compromised.

Smart contracts are a component of blockchain technology that is still relatively new. Smart contracts work in the same manner as traditional contracts do in the real world. On the blockchain, smart contracts are entirely digitally recorded. Smart contracts, in contrast to conventional contracts, are made up of computer code that is carried out by the blockchain network. Smart contracts have the advantage that, once made, they cannot be changed. This section specifies guidelines for negotiating contract terms, automatically validates the contract, and then puts the terms into effect. The execution and implementation of contracts do not necessitate any manual intervention. There are no longer any third parties necessary thanks to blockchain technology and smart contracts. By sending a contract invoking transaction to relevant contract address, such a system carries out complex programme operations. The smart contract the automatically execute the predefined terms in the secure container. When the parameters fulfil the smart contract's set conditions, the action is carried out according to the smart contract's terms.

4.2 MARKET SIZE OF BLOCKCHAIN IN HEALTHCARE

1.According to the report of Mordor intelligence, blockchain market of healthcare had value of USD 2.12 billion in 2020 in expectation to reach to USD 3.49 billion by 2026, with CAGR of 8.7% during the forecast period, 2021-26. According to GLOBE NEWSWIRE's global blockchain analysis, the global Blockchain in Healthcare market's expectation is to grow at a CAGR of 36.2 percent from USD 354.9 million in 2020 to USD 3126.8 million in 2027, up from USD 354.9 million in 2020. The increased desire to streamline company operations and the demand for supply chain management solutions that are tied to blockchain technology will drive the overall blockchain sector. APAC and MEA, for example, offer a plethora of unexplored and undiscovered blockchain opportunities.



2. The blockchain is a digital ledger that has already attracted a lot of interest in the healthcare industry. In fact, blockchain is one of the top 5 objectives for 40% of health executives. Additionally, a survey by BIS Research projects that by 2025, the worldwide healthcare market spend on blockchain will be, $5.61, billion. By 2025, the implementation of blockchain technology could save the healthcare sector between $100 and $150 billion, annually in expenditures associated to data breaches, IT, operations, support functions, and staff, as well as a decline in fraud and fake goods.

4.3 KEY PLAYERS IN THE MARKET:

The key players covered in the blockchain technology in the healthcare market report are

- IBM Corporation
- Microsoft
- Guardtime
- PokitDok, Inc
- Gem
- Global Hospital & Healthcare Management
- Chronicled
- iSolve, LLC
- Patientory
- Factom
- Medicalchain SA
- Proof.Works; Blockchain AI Solutions Ltd
- BurstIQ
- Doc.ai , Inc
- Intellectsoft US

- Medtronic
- Quest Diagnostics Incorporated
- Hong Kong Applied Science and Technology Research Institute Company Limited (ASTRI)
- Nebula Genomics; among other domestic and global players

4.4 MARKET SEGMENTATION:

- **Blockchain Technology in Healthcare Network Type Outlook (Revenue, USD Million, 2017 - 2030)**
    - Private
    - Public
    - Other

- **Blockchain Technology in Healthcare Application Outlook (Revenue, USD, Million, 2017 - 2030)**
    - Clinical Data Exchange and Interoperability
    - Claims Adjudication and Billing
    - Management of supply chain
    - Clinical Trials and eConsent
    - Others

- **Blockchain Technology in Healthcare End User, Outlook (Revenue, USD Million, 2017 - 2030)**
    - Provider
    - Payer
    - Biopharmaceutical and Medical Device Company
    - Others

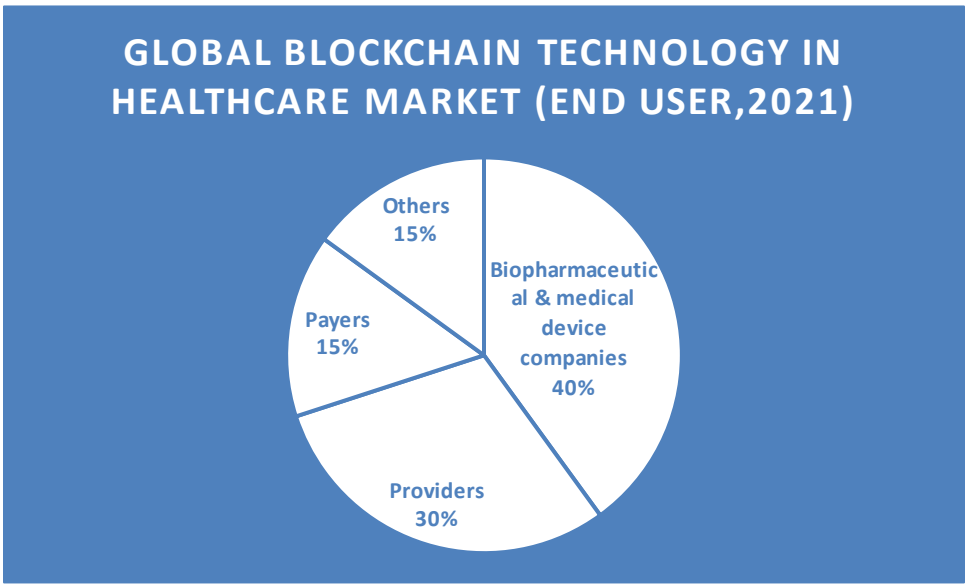


Figure: Source: grandviewresearch industry-analysis/blockchain technology healthcare market

4.5 STATISTICS ON SECURITY, PRIVACY OF ELECTRONIC HEALTH RECORDS

1. According to the article by K.T. Win, only 39% of clients believed their healthcare information was safe and secure and rest 61 % were dicey about it.

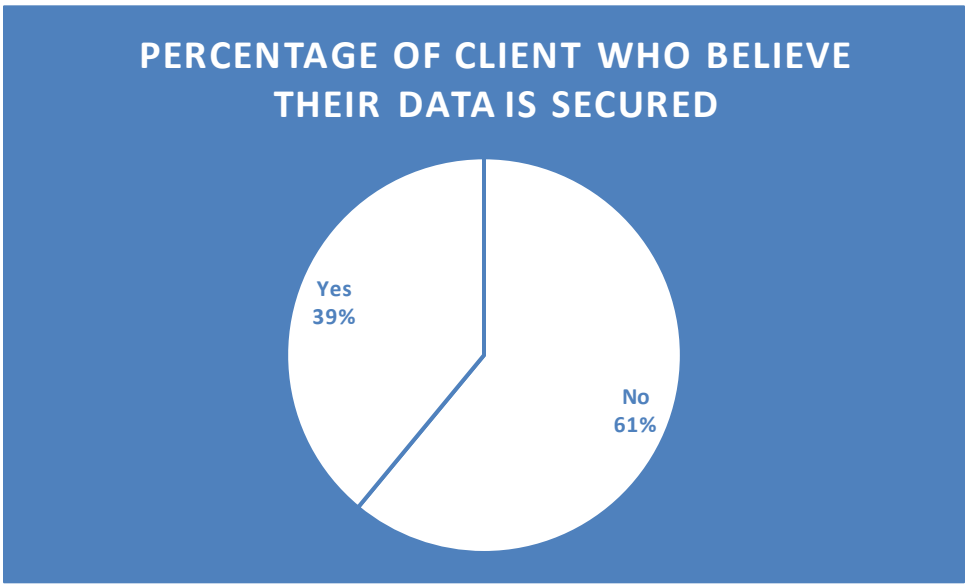


Figure: Source: "Security and privacy of electronic health records: Concerns and challenges, Science direct, 2020"

2. According to the article by K.T. Win, 66% of clients showed concerned about the privacy of their personal health records, and only 39% believed their information was safe and secure.

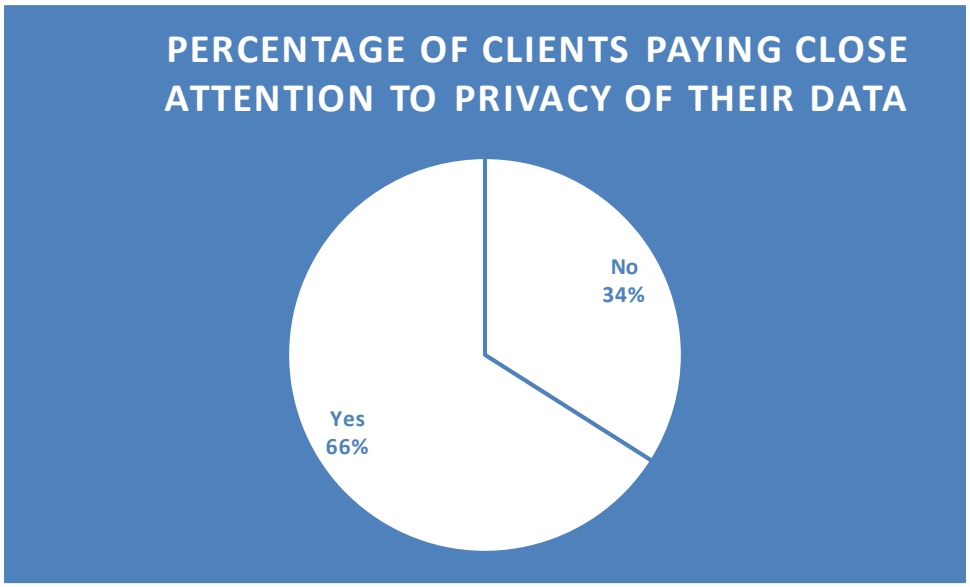


Figure: Source: "Security and privacy of electronic health records: Concerns and challenges, Science direct, 2020"

4.6 Only certified healthcare professionals will be able to access these EHRs thanks to smart contracts. Individuals/patients will be in charge of their medical information. To gain access to patient data, hospitals or research institutes will need an encrypted key. The patient will be able to choose who has access to his information and for how long.

Source: Pubmed Central

4.7 APPLICATION OF BLOCKCHAIN IN EHR:

A medical record used to be only a compilation of information that was retained for administrative, financial, scientific, and therapeutic purposes. It could only be used by one person at once and had severe accessibility restrictions. Everything might have taken anything from 1 to 6 months or more to finish because it was hand updated. Many of the issues brought on by inaccurate prescriptions, doses, and procedures are eliminated when records are clear. Additionally, adverse pharmacological reactions can be significantly decreased by integrating EHRs with drug banks and pharmacies. Limiting the prescription and ordering of medications for which there has been a documented adverse reaction in a particular patient will help achieve this. The ability to access information at any time and from any location is also useful. They may be kept indefinitely and require minimal storage space. Researchers benefit from them because they decrease the quantity of records lost, offer a comprehensive set of backup records at a cheap cost, speed up data transfer, and are economical. As a result, EHR promotes better patient care and data accessibility.

Individual EHRs are currently unstructured and managed by health care providers in their separate central databases. These databases are insecure, lack interoperability, and are easily hacked. Despite the fact that computers are found in almost every medical facility and mobile phones are carried in nearly everyone's pockets. We're still having problems getting our medical records together, exchanging them, and sharing them with a new doctor. The largest problem that healthcare systems confront today is sharing medical data amongst different healthcare providers while ensuring the privacy and integrity of the patient's data. In some parts of the world, the healthcare system is not yet fully digital. Many healthcare providers still use the old method of writing prescriptions on paper and graphing them. In this situation, both patients and healthcare providers will find it difficult to refer to these prescriptions when they are needed in the future. Interoperability is lacking in the healthcare system, which operates in silos. Even inside the same hospital, different departments' healthcare systems are unable to communicate with one another. It becomes difficult for the patient to get and discuss his clinical history with the new service

provider. To determine the specific problem, all diagnostic tests must be repeated, resulting in a delay in therapy and subsequent worsening of the disease. When a doctor is treating a patient who need immediate medical attention, it is impossible for him to determine whether the patient is allergic to any specific medication. The clinician must exercise extreme caution and do drug allergy testing to confirm this, as the consequences of administering any medicine to which the patient is allergic can be fatal. For hospital pharmacists, having a clear view of the patient data is practically impossible. As a result, predicting the inventory required to meet the needs of the hospitals becomes difficult. Every time a patient consults online, he must fill out his whole medical history. Through remote technologies, there is no practical mechanism for patients to exchange their health data with their healthcare professional.

4.7.1 Data security & Immutability

Security breaches happen when private health information is disclosed to third parties without the person's permission or authority. Theft of hardware and computers used for data storage as well as inappropriate employee usage or insider employee misconduct were the most frequent causes of security issues in the early years of EHRs. Some of the threat categories include insider use, administrative, technological, physical, and portable devices. New security issues and methods for obtaining sensitive medical data have emerged in recent years as cybercriminals' skills have increased. The healthcare sector is no stranger to threats and breaches. The growing cyber risks that digitization has brought to their operations have not been kept up with by the healthcare sector, like other industries. Additionally, compared to businesses in other sectors like banking or retail, healthcare organisations invest less in cyber security. Lack of follow-up has led to an increase in the emphasis and vulnerability of cyberattacks. At Howard University Hospital, more than 34,000 patients' names, addresses, social security numbers, medical diagnosis information, and Medicare cards were taken in two separate security incidents in 2013. When asked whether they had recently experienced a serious security incident involving both internal and external threats, 68% of healthcare firms in the United States responded positively. According to a Khin Than Win article, patient information was made public on the internet, and the names of 4000 patients who tested positive for HIV were given to Florida media. The University of Washington Medical Center's computer system was hacked, and information on 5000 patients in the fields of cardiology and

rehabilitation medicine was taken. The names of deceased kidney donors were accidentally made public by the University of Minnesota.

Nowadays, blockchain is widely acknowledged as one of the most reliable data security techniques. Rapid developments in digital technology have given birth to new problems with data security. When building a secure data network, a distributed ledger system's high level of security is helpful.

. Blockchain technology is used by businesses that supply consumer goods and services to maintain track of client information. Blockchain technology can handle any situation and ensure that data is not tampered with in any way. It is easy to perform proper validation because it is encrypted by nature. The information can only be decrypted with the help of a key provided by the person supplying it. As the name implies, blockchain is a collection of digital blocks that each contain unique data. The data cannot be tampered with from a single computer because it is not stored in a central location. Each block is linked to the blocks before and after it. Normally, hackers access information through a central point of contact where all of the data is stored, but blockchain makes this difficult for hackers, ensuring data security.

It is nearly impossible to modify data after it has been recorded inside a blockchian, making it tamper-proof and immutable. After each transaction, a new block is created that contains all of the transaction's relevant data. After that, the block is forwarded to each node, which verifies it. The block is added to the blockchain once the verification is completed. Consensus is the process of these participating nodes verifying and validating blocks. If a certain node tampers with the block, it will be removed.

4.7.2 Privacy

Justices Samul Denis Warren and Lois Brandis described privacy, the right "to be left alone." The right of individual to prevent personal information being divulged to others, as defined by Richard Rognehaugh; claim of people to free of interference by another individual, organisations, or the government. Information about patient can be shared with others with the patient's consent only or as required by law. When patient is not able to make decision about information to be share due to age or mental incompetence, the patient legal representative or legal guardian should do so on his or her behalf. Many surveys have showed a high level of concern regarding health information privacy. Nearly 66 percent of clients were concerned about the privacy of their personal health records, according to an article by Ismail Keshta and Ammar Odeh, with only 39 percent trusting that their information was secure and protected. Many people believe that sharing their medical information would put their privacy in jeopardy. Rising concerns about the privacy of medical data have a negative impact on patients' willingness to share their health information online. Patients' sensitive personal information about infertility, abortion, and sexually transmitted illnesses, among other things, could have an impact on their mental health if it is accessed by other stakeholders in the EHR. If EHRs are to function correctly, organisations for health care, insurance companies, and other will need access to the data. Protecting privacy require limiting access to information to just those who are authorised. The first step is to grant users access to system.

Each patient will have a distinct identity on the blockchain network, and his clinical data will be periodically linked to this identity as an EHR digital asset. The use of blockchain technology will allow people to manage their electronic health records (EHRs). It appears to be possible to create a secure system using access control and blockchain technology. Patients can pre-define access rights (authorise, deny, revoke), operations (read, write, update, delete), and time for sharing their data using smart contracts on the blockchain without losing control. When all the prerequisites are completed, smart contracts will be implemented on the blockchain and offer an audit mechanism for each request entered into the ledger. Only approved healthcare professionals would be able to access these EHRs thanks to smart contracts. Individuals/patients will be in charge of their medical

information. To gain access to patient data, hospitals and research organisations will need encrypted keys. The patient will be able to choose who has access to his information and for how long. Individuals can also provide their consent for healthcare providers to examine their information in the event of an emergency.

4.7.3 Interoperability

Interoperability refers to a system's capacity to share data with other systems. Two EHR systems must be able to share and then use data in order to be truly interoperable. Across the country, a significant variety of government-certified EHR solutions are in use, each with its own technological specifications, functional capabilities, and clinical nomenclature. Because of these differences, developing a standard data-transfer interoperability format is difficult. Because EHR systems are usually substantially customised to a company's specific workflow and preferences, they are not always compatible when built on the same platform. Interoperability refers to the ability of two EHR systems to interchange information and use data.

On the blockchain network, each patient will have a unique identity, and his clinical data will be connected to this identity as an EHR digital asset at various stages. Blockchain has the potential to create a truly interoperable network. Whenever a patient has a diagnostic test or consultation, the information is added to the patient's own electronic health record. Health-related data gathered by smart devices can also be safely incorporated into it. As and when needed, this EHR data can be conveniently shared among other health providers. This might even lower the cost of healthcare by obviating the need for a duplicated diagnostic test. On the basis of this exact data, the healthcare professional may deliver better patient care.

4.8: The challenges in HER and how it can be overcome using blockchain technology:

Challenges in EHR	**Benefits of blockchain technology**
Data security & Immutability	Distribution of the encryption key When compared to EHR security, ledger technology ensures that data is more secure. The previous and subsequent blocks are linked. Any change to any of the blocks will result in a change in the hash number. As a result, it is unchangeable.
Privacy	Removes the need for a third party. Smart contracts ensure that data can only be used or viewed by those who meet the conditions set out in the smart contract. To access patient data, hospitals and research groups need encrypted keys.
Interoperability	Data from EHRs can thus be easily shared among different health providers as needed. Data can be accessed by several healthcare departments. Oxygen saturation level, BPM, BP, daily step count, calorie consumption, and other data integrated with patient electronic health record to help doctors give better consultation. The risk of prescribing the wrong medicine to a patient is reduced when EHR data is interoperable. It would also lower hospital and healthcare provider overhead costs.

CONCLUSION (CHAPTER 5)

Despite the benefits of EMRs, future of health care requires the risks should be identified and successfully managed. Privacy, interoperability, data security, and immutability are just a few of the issues that blockchain can help with. When blockchain is paired with encrypted keys and smart contracts, patient data is kept private and secure. Because blockchain is based on distributed ledger technology, it has the features of decentralisation, distributed ledger, and immutability. Electronic health records on blockchain will serve as a single and integrated backbone for the healthcare industry once implemented.

SUGGESTIONS (CHAPTER-6)

The new technology needs have emphasized how crucial it is for businesses to be future-ready in order to provide customers with a revolutionary experience. In reality, pandemic like also Covid's influenced has caused people to see that insurance is no longer a priority but rather a necessity. Additionally, customers of today are well-connected, quick to react, and unafraid to accept new technology that can significantly enhance their lives.

The next stage in empowering end users will be to integrate blockchain technology into EHRs. Customers can view their transactions and give permission to their insurance agent, doctor, or pharmacist if they want to look at their records. Additionally, blockchain technology would assure operational efficiency, transparency, and prevent cyber-hacking.

Before making the necessary infrastructure investments, team members and decision-makers should be taught on the disruptive potential of implementing blockchain in electronic health records (EHRs).

Although implementing such technologies may seem time-consuming and expensive, doing so is ultimately best for the general public's health. The genuine benefit in industry is anticipated to come from working together on a single platform to provide true interoperability capabilities that did not previously exist with the widespread adoption of blockchain technology. Blockchain technology has revolutionised electronic health records (EHRs).

REFERENCES (CHAPTER -7):

7.1 Shahnaz A, Qamar U, Khalid A. Using blockchain for electronic health records. IEEE Access. 2019 Oct 9;7:147782-95.

7.2 Tanwar S, Parekh K, Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. Journal of Information Security and Applications. 2020 Feb 1;50:102407.

7.3 Ekblaw A, Azaria A, Halamka JD, Lippman A. A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data. InProceedings of IEEE open & big data conference 2016 Aug 13 (Vol. 13, p. 13).

7.4 Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. InAdvances in computers 2018 Jan 1 (Vol. 111, pp. 1-41). Elsevier.

7.5 Capece G, Lorenzi F. Blockchain and Healthcare: Opportunities and Prospects for the EHR. Sustainability. 2020 Nov 20;12(22):9693.

7.6 Dimitrov DV. Blockchain applications for healthcare data management. Healthcare informatics research. 2019 Jan 31;25(1):51-6.

7.7 Girardi F, De Gennaro G, Colizzi L, Convertini N. Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain. Electronics. 2020 Jun;9(6):884.

7.8 Mayer AH, da Costa CA, Righi RD. Electronic health records in a Blockchain: A systematic review. Health informatics journal. 2020 Jun;26(2):1273-88.

7.9 Angraal S, Krumholz HM, Schulz WL. Blockchain technology: applications in health care. Circulation: Cardiovascular quality and outcomes. 2017 Sep;10(9):e003800.

7.10 Onik MM, Aich S, Yang J, Kim CS, Kim HC. Blockchain in healthcare: Challenges and solutions. InBig data analytics for intelligent healthcare management 2019 Jan 1 (pp. 197-226). Academic Press.

7.11 Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences—A scoping review. International Journal of Medical Informatics. 2020 Feb 1;134:104040.