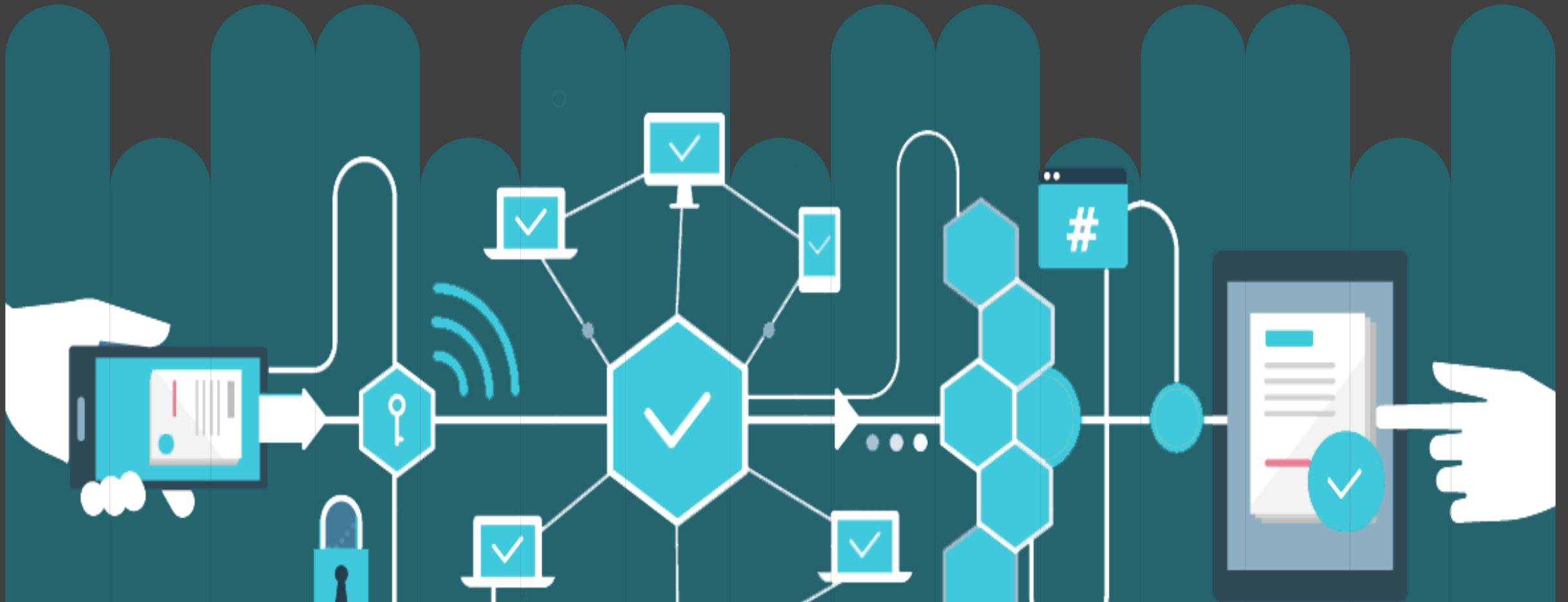




BLOCKCHAIN BASED SOLUTION FOR ELECTRONIC HEALTH RECORDS

ADITYA SINGH
ROLL NUMBER-0867
IIHMR UNIVERSITY JAIPUR

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.
- 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.
- The European Union nations aimed to have a single health system in place by 2015.

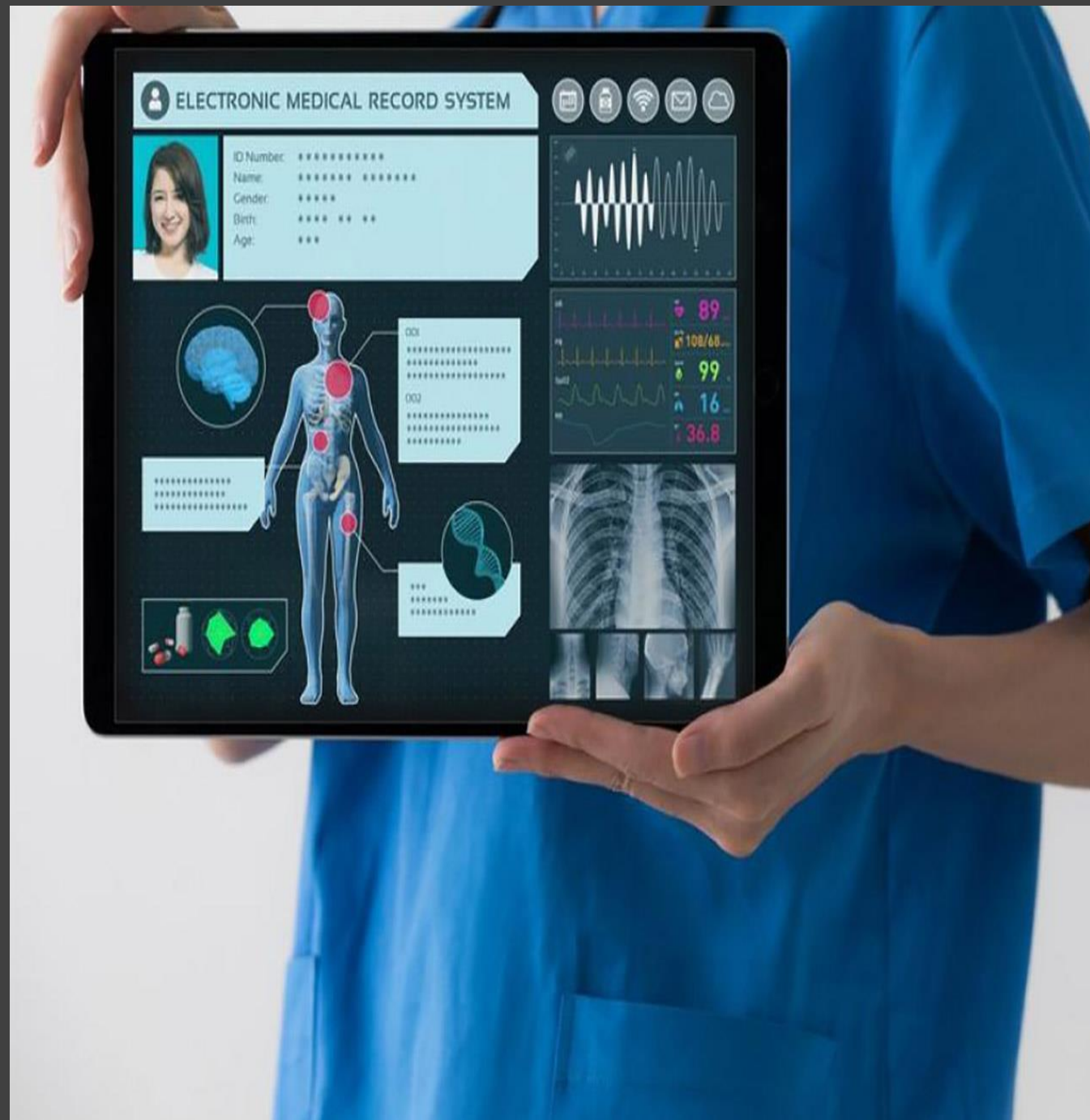


WHAT IS ELECTRONIC HEALTH RECORD?

- 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.
- An EHR contains valuable and pertinent automated medical information, including: Patient vitals, prescriptions, medical histories, diagnoses, surgical notes, discharge summaries

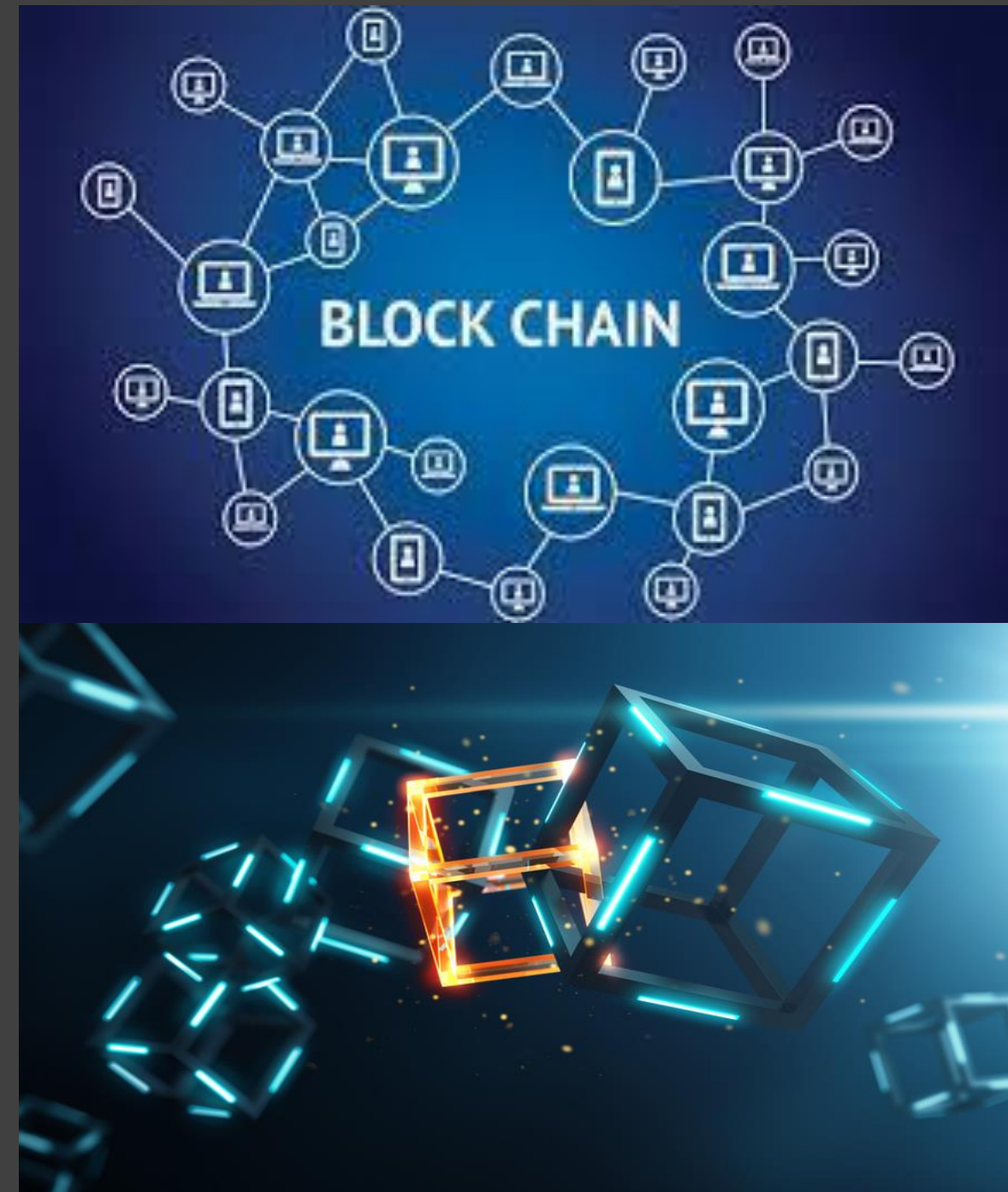
BENEFITS-

- ✓ Better quality of patient care
- ✓ Better emergency care
- ✓ Reduction in medical errors
- ✓ Increased efficiency & productivity
- ✓ Cost savings
- ✓ Large amount of data can be stored
- ✓ Reduced chances of losing records



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.
- 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.
- The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT).
- 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 invention of the blockchain for bitcoin made it the first digital currency.



BLOCKCHAIN APPLICATION IN CYPTOCURRENCY

- Bitcoin (₿) is a decentralized digital currency without a central bank or single administrator, that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.
- Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger also known as blockchain.
- 1 Bitcoin equals \$ 34,127 (₹ 25,51,210.4)
- On 9th June 2021 El Salvador adopted Bitcoin as a legal tender.

Current blockchain systems are categorized into four types-

- Public
- Private
- Consortium
- Hybrid



4 types of **blockchain** networks



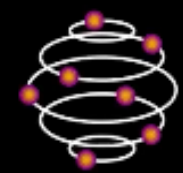
Consortium blockchains



Semi-private blockchains



Private blockchains



Public blockchains

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.

”

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

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

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.



LITERATURE REVIEW

- In a study undertaken by Amit Sharma, Praveen Aggarwal, Fouzia.F.Ozair and Naver, the objective of the study was 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.
- In a study conducted by B. A. Saranga Jayawardena, the aim was 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.

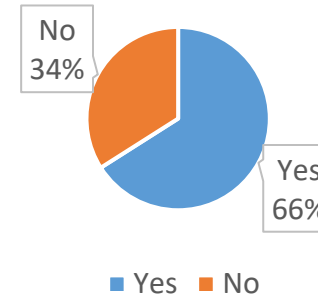
LITERATURE REVIEW

- In a 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.
- The study was undertaken 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.

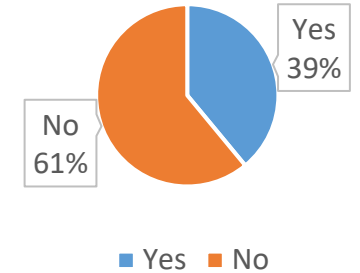
FINDINGS

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

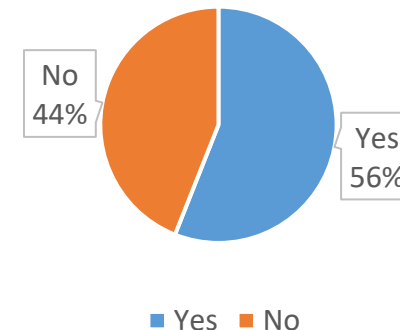
Clients paying attention to data privacy



Percentage of clients who think their data is secure

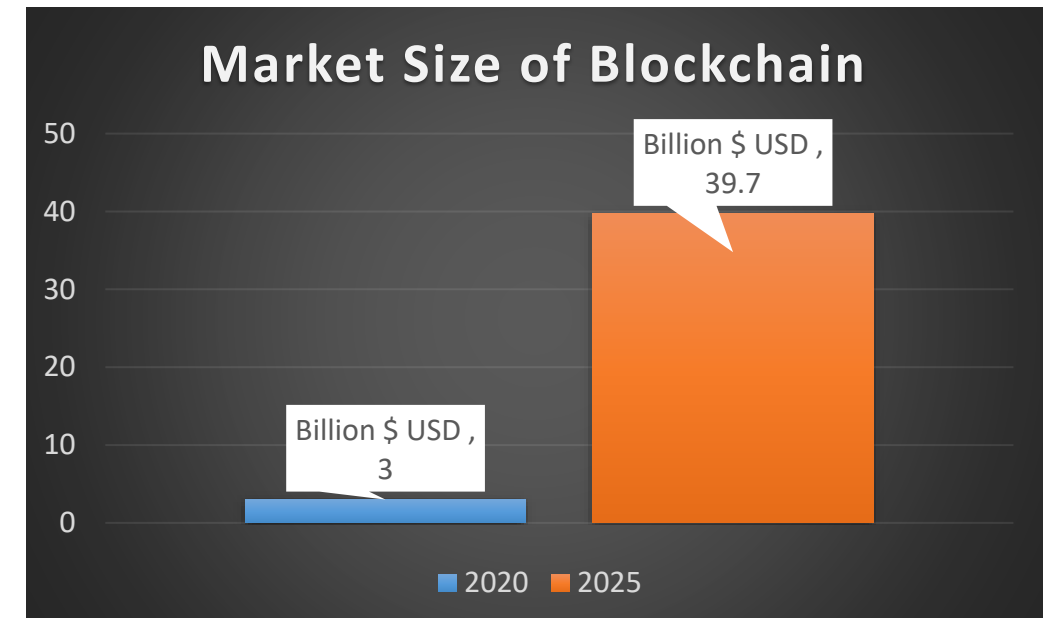
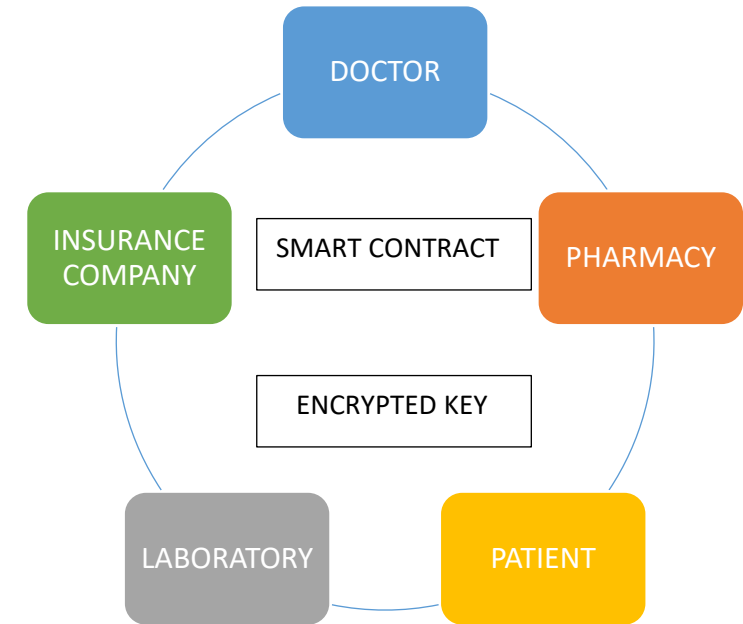


Percent of healthcare stakeholders who intend to implement blockchain by 2020



FINDINGS

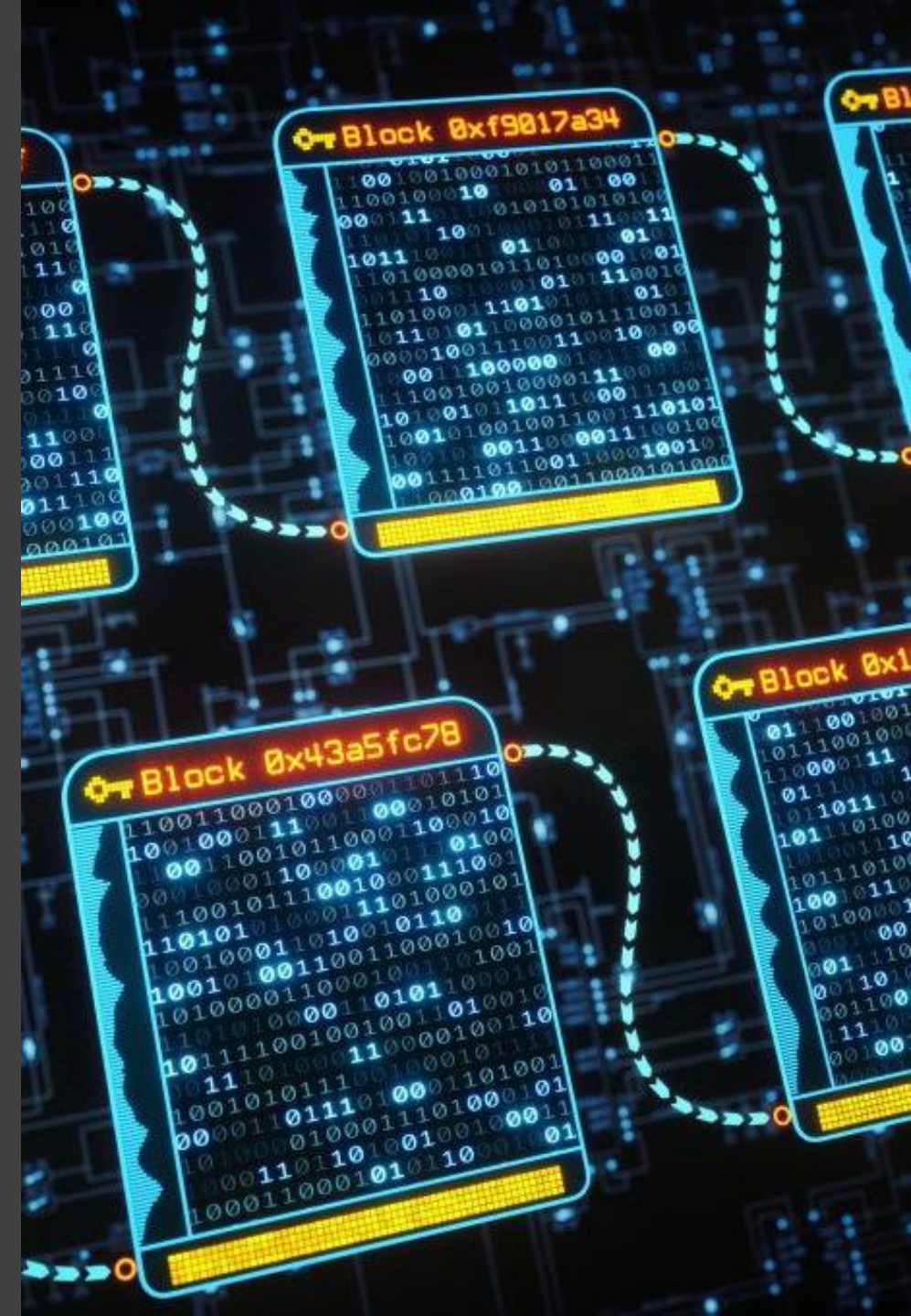
- Smart contracts will ensure that only authorized healthcare providers can access these EHRs. The individuals/patients will be the owners of their medical data. The hospitals or research institutes will require encrypted key to get an access to the patient data. The patient will have the provision to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



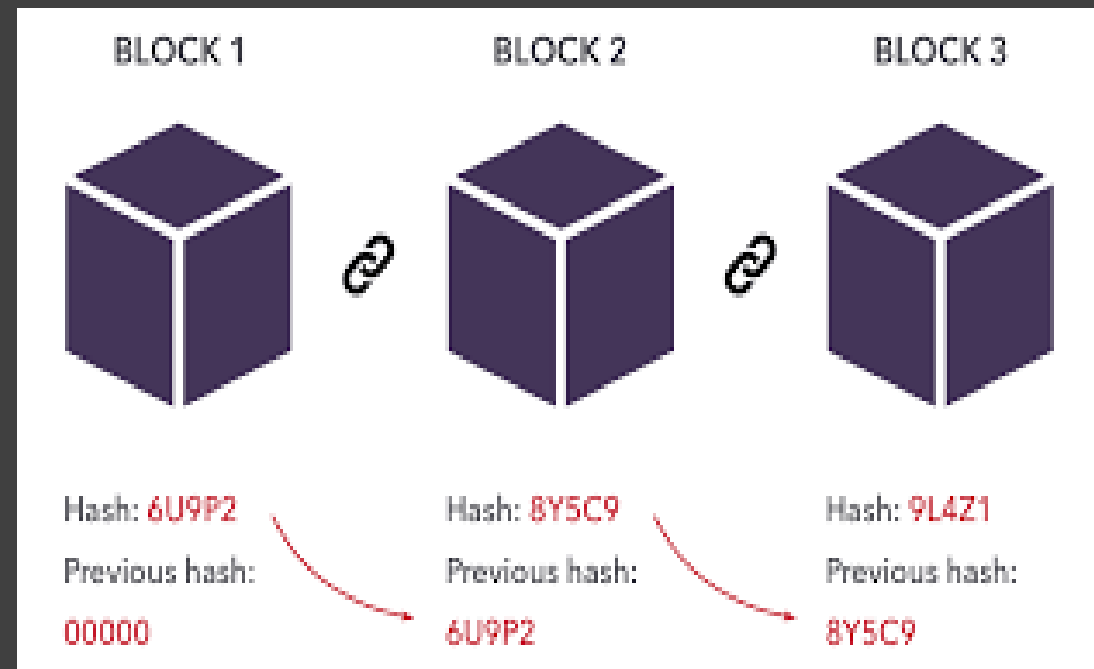
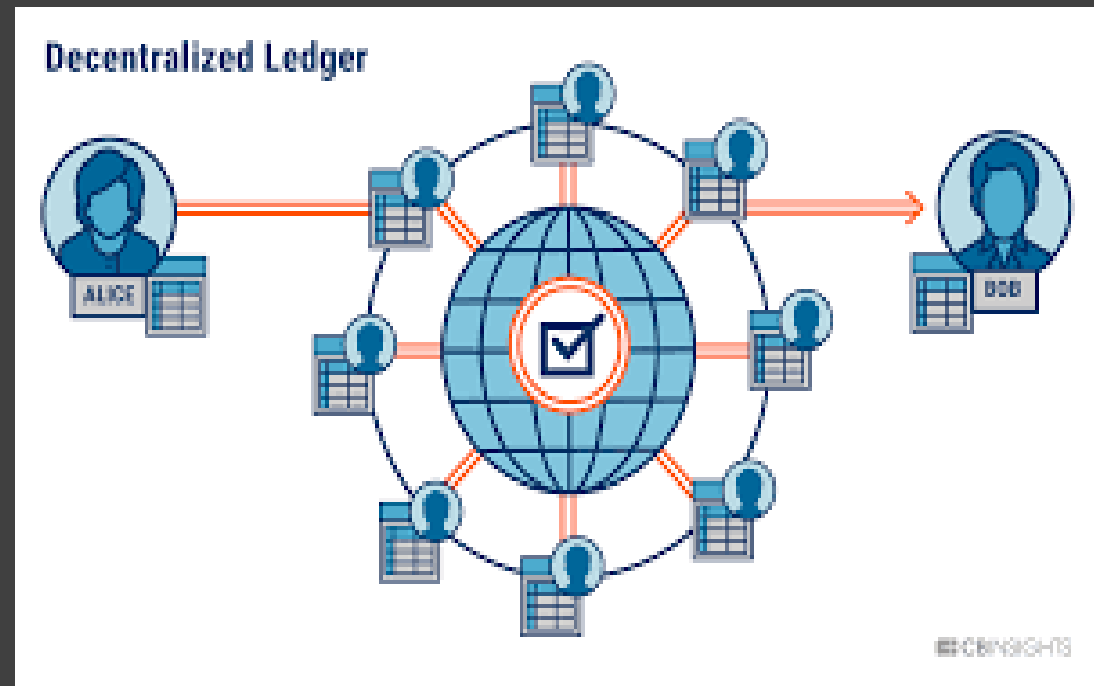
DISCUSSION

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. The main features of blockchain are:

- Decentralization- It uses peer to peer network and eliminates the need to rely on any centralized third party or middlemen to store data.
- Distributed ledger - Is the record of all transactions shared with every person on the same blockchain network. Each person gets a copy of the ledger which gets updated when a new block is added on the blockchain.
- Immutability - Once the data has been recorded inside a blockchain it becomes nearly impossible to change it, thus making it tamper proof.



- 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.
- 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. Each block also includes a hash - a unique identifier for the block and all of its contents. 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.



- Every block also has 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. 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.
- Smart contracts are a relatively new addition to the blockchain. Smart contracts are entirely digital contracts that are kept on the blockchain. They are made up of software code and are performed by the blockchain network. Once decided, these smart contracts cannot be changed or updated
- This saves contract negotiating guidelines, automatically checks the contract, and then executes the negotiated terms. They do not necessitate any manual involvement in order to execute and implement contracts. The use of blockchain in conjunction with smart contracts eliminates the need for reliance on third parties.



APPLICATION OF BLOCKCHAIN IN STRENGTHENING EHR

➤ PRIVACY

Privacy is 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.

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.

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. 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.

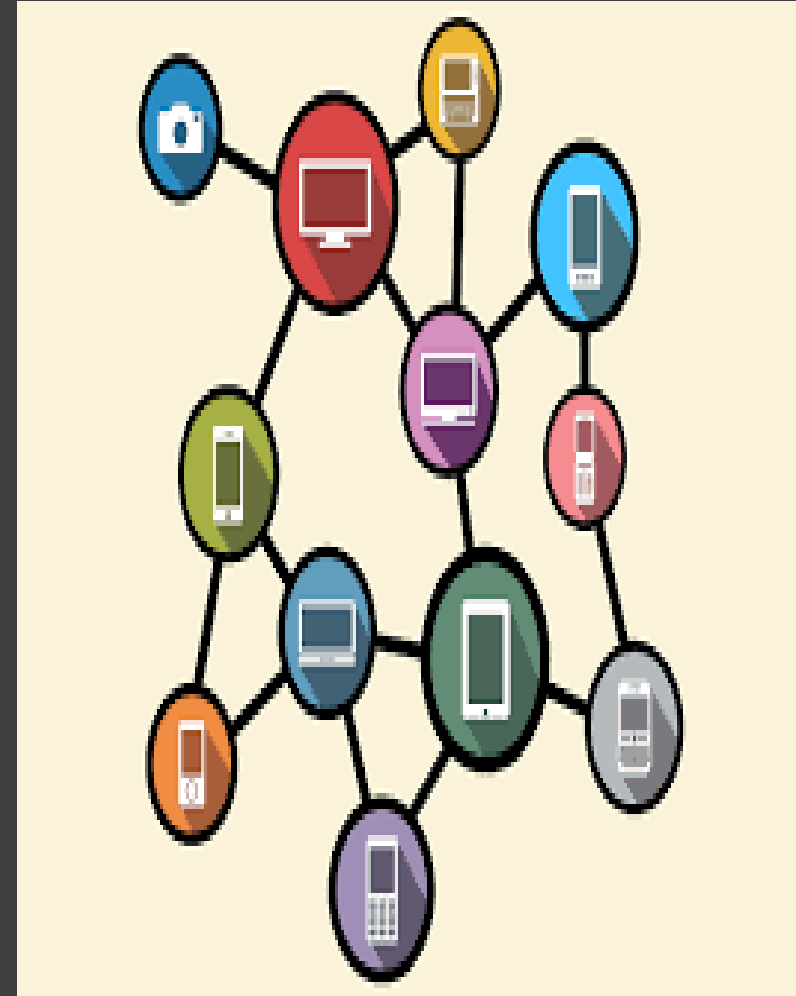


➤ INTEROPERABILITY

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.

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.

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 AND IMMUTABILITY

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 .The potential threat categories can be categorized as – administrative, technical, physical, insider use and portable devices.

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

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.



A distributed ledger system's high level of security is advantageous for building a secure data network. 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 blockchain it becomes nearly impossible to change it, thus making it tamper proof and immutable.



CONCLUSION

- Blockchain works through distributed ledger technology therefore possessing the properties of – decentralized, distributed ledger and immutability.
- 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. Once implemented the electronic health records on blockchain will serve as a common and integrated backbone for the health industry.



WAY FORWARD

The pandemic of COVID 19 has also highlighted the need of organizations being future-ready in order to provide a transformational consumer experience. Regular cyber threat attacks on EHRs and the rising importance of customer satisfaction in terms of privacy and interoperability issues are some of the challenges which are there in EHRs.

In the healthcare sector, blockchain technology will be a step forward in terms of empowering end users. While integrating such technology may appear inconvenient and pricey at first, it is in the long term in the best interests of public health. With the broad adoption of blockchain technology, the real value in business will come from working together on a single platform to enable genuine interoperability possibilities that have never existed before. The healthcare business is on the verge of advancement thanks to 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 Kravetska, 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>

