Blockchain Application in Health Record Management Systems

Mahsa Dashtizadeh
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
mahsa.1999da@gmail.com

Julia Juremi
School of Computing
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
julia.juremi@apu.edu.my

***Abstract*— With the contributions of different cutting-edge technology, healthcare systems are able to govern and keep an eye on the health of their patients. It is essential that the development of these systems have a clear and unambiguous focus on increasing the effectiveness of these systems. The distributed ledger technology known as blockchain, with its built-in consensus methods, decentralized data storage, and cryptographically protected protocols, may be used to make such systems more resilient and trustworthy. Blockchain, the technology underpinning bitcoins, offers a decentralized network to confirm transactions and guarantee that they cannot be altered once they have been recorded. Blockchain technology minimizes the dangers that are associated with having a centralized design by decentralizing the function of information validation among the peers of the network. It has the potential to transform a wide variety of commercial applications, including the data management, prediction markets, and sharing economy, among others. The primary objective of this study is to conduct literature research about blockchain applications in the healthcare industry, particularly medical record management systems. In the context of this project, 14 papers have been chosen to be looked at. This article provides a quick overview of the blockchain, including its history, advantages, uses, and security. In addition, the medical record management system, together with its history and EHRs, as well as a blockchain-based HER management system, is presented further down in this article.**

Keywords—Blockchain, Data integrity, Healthcare, Health Record management system, Traceability, Information Security

I. Introduction (*Heading 1*

When paired with ubiquitous sensing and communication technologies, the architectural paradigm of healthcare systems may improve the healthcare system in a number of ways. In this kind of designed system, cyber components like computer hardware and communication networks are added to the physical system or process to make it more effective. Because of how closely these parts are bound together, the proper operation of one cannot be achieved without the proper operation of the other.(Rathore et al., 2020).

The process of preserving and maintaining patient data is one of the most essential aspects of the healthcare sector since the patient records are considered as a really important element of healthcare industry. There are a few different approaches to writing a medical record, the most common of which is the written medical record on paper, which has been in use since 1600 BC. The more appointments a patient has had, the thicker the paper file will become. Evidently, analysing paper-based medical data via the use of computational linguistic approaches is a challenging task (Dalianis, 2018).

As it has been mentioned by Wang et al. (2020), he standard medical record keeping systems have to deal with a difficult administration method for the processing of data in order to protect the confidentiality of patients, which results in an immense waste of human resources. For the purposes of the sharing of medical records, such an architecture is manifestly inefficient. The blockchain technology has lately been used in an effort to safeguard the sharing and administration of medical data.

The confidentiality of the patients is ensured by the cryptography functionality of the blockchain networks. Having data that is both accurate and unchangeable is essential for keeping patient records secure. Blockchain technology may be thought of as a distributed database, which saves information across the network's nodes to get around the scalability issue. As a result, it offers enhanced levels of stability, uniformity, and resistance to assault (Wang et al., 2020). In this paper, a literature review on number of studies regarding the blockchain technology domain along with its applications, benefits and other sub domains is provided. Besides that, a review on the healthcare, electronic health records, and blockchain based EHR management system is performed accordingly.

II. Blockchain

Blockchain technology can be characterized as a distributed database system that is managed by numerous nodes on a peer-to-peer network. This technological solution does not need a central administrator or administration of centralized databases in order to work. Encryption and replication are used to protect the integrity of the data, which is widely dispersed among several nodes. The concept of a blockchain was first presented to the public 31 October 2008 in the form of a white paper written by Nakamoto. On a peer-to-peer network, he came up with the idea of using Bitcoins to transfer money from one person to another without going through a banking institution (Khatoon, 2020). Blockchain technology will provide a development environment for highly secure, decentralized, anonymized, audible record chains which are presently used in cryptocurrency systems (Keat & Keong, 2021; Lo et al., 2020; Loke et al., 2020; Morel et al., 2022).

Nakamoto's primary objective was to develop a trustworthy system with distributed peer to peer ledger technology that eliminates double spending by determining the transaction sequences. The word "blockchain" refers to a collection of blocks, each of which contains a collection of data from the past, present, and future. Immediately after joining the chain, each block serves an important function in connecting to the previous block and the following block. The main purpose of each block is to register, validate, and disseminate transaction data to other blocks on the blockchain. Since every block in the chain would be affected, it is impossible to remove or change a block in the chain (Khatoon, 2020).

A. *The Maturity of Blockchain Technology*

According to Bashir (2018), in 2008, a new paradigm was presented to the world in the form of the development of Bitcoin, which would result in a revolution throughout the whole human civilization. It will touch every area, such as but not only the economy, financial system, healthcare, the media and law. This technology has grown steadily in popularity throughout the globe over the years, as seen in the following graph. The accompanying graph indicates that in 2013, thoughts and views developed from uses of blockchain technology aside from cryptocurrency.

After that, in 2014, some experiments and research began, whereby some ideas and other research were proven. The blockchain technology is expected to continue undergoing adaptations and maturing while also undergoing more development. The technology is not expected to be sufficiently developed for use in day-to-day activities until 2025 at the earliest (Bashir, 2018)

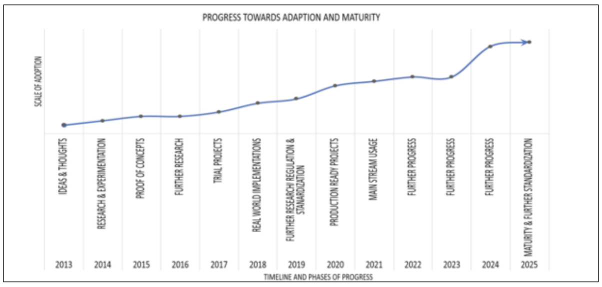


Fig. 1. Blockchain technology maturity (Bashir, 2018)

III. Blockchain Classification

The permission model of a blockchain network may be used to categorize the blockchain technologies by determining who has the authority to administer them. The permission-less blockchain, often known as the public blockchain, is the kind of blockchain that allows anybody to publish a new block. On the other hand, in private or permissioned blockchain, just a group of users are authorized to publish blocks. These two categories are broken out into more detail below (Ahmed Farah, 2018).

A. *Public or permission-less Blockchain*

One way to think of a public blockchain is as a database that is open to anybody to access and does not need any special authorization. Anyone may publish a block on this Blockchain without the necessity for regulatory clearance. It is possible to read the blockchain and perform transactions on it since everyone has the power to publish blocks. Malicious users may generate blocks that evade the infrastructure on public blockchain networks. Therefore, w hile attempting to publish a block, public blockchains commonly utilize a multiparty contract that forces users to either enhance or conserve resources (Yaga, Mell, Roby and Scarfone, 2018).

B. *Private or permissioned Blockchain*

Individuals may only publish blocks on private blockchain networks after being granted permission to do so by a certain authority. It is feasible to restrict read access and to regulate who may conduct transactions as a result of the fact that these blockchains are only maintained by users who have been granted permission to do so. As a result, private blockchain networks may either allow anybody to access the Blockchain or restrict access to just those who have been granted access.

These blockchain networks can offer the same traceability and decentralized, resilient, and robust storage of data as public ones. permissioned blockchain networks provide transparency and analysis that may aid in guiding corporate choices and holding irresponsible people accountable (Ahmed Farah, 2018).

IV. Blockchain Essential Components

A. *Cryptography*

According to Sahu (2021), cryptography can be described as the practice of designing techniques and protocols that prevent a third party from seeing and gaining information of private material in a transmission. Kryptos and Graphein are the ancient Greek terminology for cryptography. The Greek words kryptos, for "hidden," and graphein, for "to write," form the word cryptography. The four most essential concepts in cryptography are key, cypher, decryption and encryption. The goal of encryption is to convert an actual text or regular text into a randomized sequence of bits called ciphertext.

The process of decryption, on the other hand, might be thought of as the inverse of encryption; more specifically, it is the transformation of encrypted material into plain text. The mathematical equation that is used in the process of transforming plain text into ciphertext is referred to as a cypher. Key is the minimum amount of data required for encryption and decryption. The three main subcategories of cryptography are known as hash functions, symmetric key cryptography and asymmetric key cryptography. The next section will go over the two primary categories of cryptographic algorithms that are used by blockchain technology. (Sahu, 2021).

B. *Asymetric key Cryptography*

As it has been mentioned by Yaga, Mell, Roby and Scarfone (2018), asymmetric-Key Cryptography, as opposed to Symmetric-Key Cryptography, utilizes two different keys for decryption and encryption which are called a private key and a public key that are mathematically related with each other. It is possible to share the public key with the general public without compromising its secrecy, but the private key must be kept secret for reasons of safety and privacy. No matter how closely two keys are connected, it is impossible to reliably compute the private key using just the public key.

The private or public key may be employed to encrypt, while the other key can be used to decrypt. To build the confidence among strangers in this framework, the contracts are "digitally signed." This entails encrypting a transaction using a secret key so that only those holding the public key may decode it. The private key assures that the private key is accessible by the transaction’s signer since the public key is freely available. Another option is to encrypt the data using the user's public key, which would then allow the data to be decoded only by those individuals who have access to the user's private key (Yaga, Mell, Roby and Scarfone, 2018).

C. *Cryptographic Hash Functions*

The blockchain technology relies heavily on the cryptographic hash function as an important component. Hashing may be described as the application of a cryptographic hash function to data that generates a unique result for every input regardless of its size. It is possible to refer to this output as a message digest, or just digest. It enables anyone to independently enter data, hash the information, and retrieve the identical result, indicating that the data has not been altered. A totally new digest may be generated even if just a single component of input is changed.

Blockchain networks employ cryptographic hash functions in a variety of ways. Within the context of blockchain technology, the protection of block data is the fundamental purpose of hashing. Using blockchain technology, a publishing node will hash the transaction data, that will be stored on the block header. In the future, the blockchain network's header will be encrypted utilizing a hash function as well, ensuring security against hackers and attackers. Additionally, this method may be used to derive addresses and generate unique IDs (Yaga, Mell, Roby and Scarfone, 2018).

D. *Transactions*

On a blockchain, two or more entities engaging in a mutual exchange might be referred to as a transaction. In the case of cryptocurrencies, for example, a transaction symbolizes the exchange of cryptocurrency between two nodes of the blockchain network. Tracking actions on digital or physical resources may be the basis for a transaction in business-to-business scenarios (Yaga, Mell, Roby and Scarfone, 2018).

E. *Blocks*

To begin, a blockchain network user transmits the necessary transaction to the blockchain via the system. This transaction is then published to all nodes in the blockchain network later on. When a waiting transaction is propagated among peers, it must wait in a queue before it can be placed into the blockchain for many blockchain systems. Transactions may be added to the ledger after a block has been published by a publishing node on the network. The block header and block information are both included in a block. Fig 2. Shows Blocks and block-chaining.

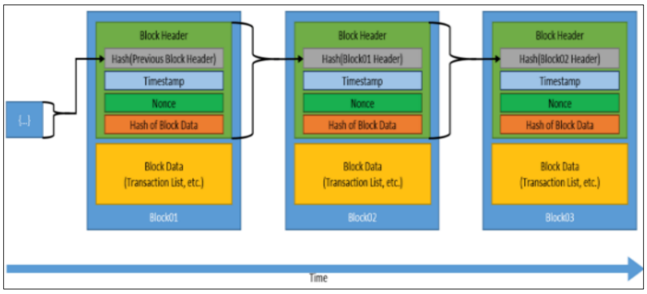


Fig. 2. Blocks and block-chaining (Yaga, Mell, Roby and Scarfone, 2018)

Each block's information may be found in the header of the block. Hash of preceding block's header, block number, hash of current block's contents, a timestamp, and block size are all included in this information.

The hash value of a previously published block will change if it is updated. This makes it possible to easily identify and dispose of any blocks that have been changed. The following illustration depicts a typical sequence of blocks included inside a blockchain (Yaga, Mell, Roby and Scarfone, 2018).

F. *Smart Contracts*

These programs are being executed on the blockchain and include the organization's justification for certain actions. They are dynamically executable and capable of being acted upon. While the smart contract capability is not available on all blockchain networks, it has become a highly desirable feature for blockchain implementations because of its adaptability and power. Smart contracts have a variety of applications, including but not limited to identity management, financial markets, e-governance, data management, insurance and commercial finance (Bashir, 2018).

G. *Address*

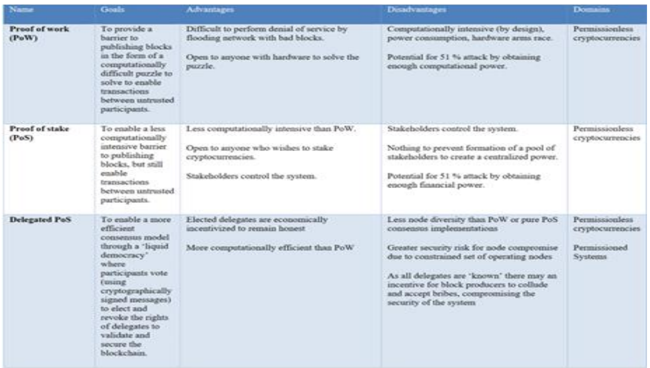
As it is mentioned by Yaga, Mell, Roby and Scarfone (2018), in a blockchain transaction, the sender and recipient are identified by their addresses. A cryptographic hash function of a network user's public key yields an address, which is a short string of alphanumeric letters. Public addresses, as contrast to private keys, are readily accessible to the whole public. Addresses are typically formed by applying a cryptographic hash function to a created public key and then converting the result to text.

H. *Consensus Model*

The ability to determine who gets to submit the next block is a key feature of the blockchain. This is accomplished by using one of the conceivable consensus models. In permissionless blockchains, there are usually many nodes fighting to publish the next block at the same time. As with private blockchain networks, there may be some level of trust between nodes (Yaga, Mell, Roby and Scarfone, 2018).

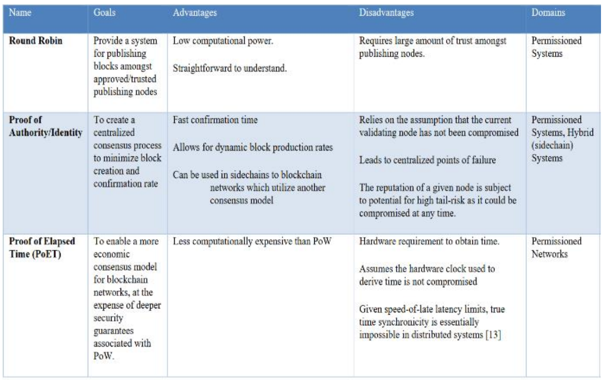
In this circumstance, a resource-intensive form of consensus, such as computation time, may not be required to determine which member enters the next block into the chain. For particluar private blockchain implementations, a consensus strategy goes beyond just verifying the validity and authenticity of the blocks, and instead necessitates testing and confirming the validity and authenticity of each transaction from conception to final block placement. Table I and II. shows few comparisons of consensus models' properties.

TABLE I. CONSENSUS MODELS 1 (YAGA, MELL, ROBY AND SCARFONE, 2018)



Name	Goals	Advantages	Disadvantages	Domains
Proof of work (PoW)	To provide a barrier to publishing blocks in the form of a computationally difficult puzzle to solve to enable transactions between untrusted participants.	Difficult to perform denial of service by flooding network with bad blocks. Open to anyone with hardware to solve the puzzle.	Computationally intensive (by design), power consumption, hardware arms race. Potential for 51 % attack by obtaining enough computational power.	Permissionless cryptocurrencies
Proof of stake (PoS)	To enable a less computationally intensive barrier to publishing blocks, but still enable transactions between untrusted participants.	Less computationally intensive than PoW. Open to anyone who wishes to stake cryptocurrencies. Stakeholders control the system.	Stakeholders control the system. Nothing to prevent formation of a pool of stakeholders to create a centralized power. Potential for 51 % attack by obtaining enough financial power.	Permissionless cryptocurrencies
Delegated PoS	To enable a more efficient consensus model through a 'liquid democracy' where participants vote (using cryptographically signed messages) to elect and revoke the rights of delegates to validate and secure the blockchain.	Elected delegates are economically incentivized to remain honest More computationally efficient than PoW	Less node diversity than PoW or pure PoS consensus implementations Greater security risk for node compromise due to constrained set of operating nodes As all delegates are 'known' there may an incentive for block producers to collude and accept bribes, compromising the security of the system	Permissionless cryptocurrencies Permissioned Systems

TABLE II. CONSENSUS MODELS 2 (YAGA, MELL, ROBY AND SCARFONE, 2018)



Name	Goals	Advantages	Disadvantages	Domains
Round Robin	Provide a system for publishing blocks amongst approved/trusted publishing nodes	Low computational power. Straightforward to understand.	Requires large amount of trust amongst publishing nodes.	Permissioned Systems
Proof of Authority/Identity	To create a centralized consensus process to minimize block creation and confirmation rate	Fast confirmation time Allows for dynamic block production rates Can be used in sidechains to blockchain networks which utilize another consensus model	Relies on the assumption that the current validating node has not been compromised Leads to centralized points of failure The reputation of a given node is subject to potential for high tail-risk as it could be compromised at any time.	Permissioned Systems, Hybrid (sidechain) Systems
Proof of Elapsed Time (PoET)	To enable a more economic consensus model for blockchain networks, at the expense of deeper security guarantees associated with PoW.	Less computationally expensive than PoW	Hardware requirement to obtain time. Assumes the hardware clock used to derive time is not compromised Given speed-of-late latency limits, true time synchronicity is essentially impossible in distributed systems [13]	Permissioned Networks

V. BENEFITS OF BLOCKCHAIN

A. *Trust and Transparency*

The fact that blockchains are decentralized and that anybody may see the data stored on them contributes to the transparency of the system. As a direct result of this, trust is built. This is more appropriate in instances when human choice in benefit selection must be restricted, such as the release of cash or incentives (Bashir, 2018).

B. *Decentralization*

This is a fundamental tenet of the blockchain and one of its primary benefits. It is not necessary to use the services of a reliable third party or broker to verify transactions. Alternatively, a consensus mechanism may be used to agree on the legitimacy of transactions (Bashir, 2018).

C. *High Availability*

This system is very accessible due to the fact that it is built on millions of peer-to-peer network nodes and the content from each node is spread and examined. Although some nodes fail or become inaccessible, the network as a whole continues to operate and remains highly useful. The excellent usability is a direct result of this redundancy (Bashir, 2018).

D. *Hgihly Secure*

The contents and headers of each block are hashed using a cryptographic algorithm, which is one of the reasons why blockchain networks are regarded as the most secure kind of network (Bashir, 2018).

E. *Immutability*

Once data has been published to the blockchain, it is very hard to make changes to it again without affecting the whole system. It is feasible to say that blockchain is an immutable database despite the fact that some of its entries might been changed; this is due to the fact that changing these records is very difficult and almost impossible (Bashir, 2018).

F. *Cost Saving*

As a result of the fact that the blockchain model does not need a reliable third party or clearing house, it is possible that overhead expenses, such as the fees given to these parties, may be greatly reduced (Bashir, 2018).

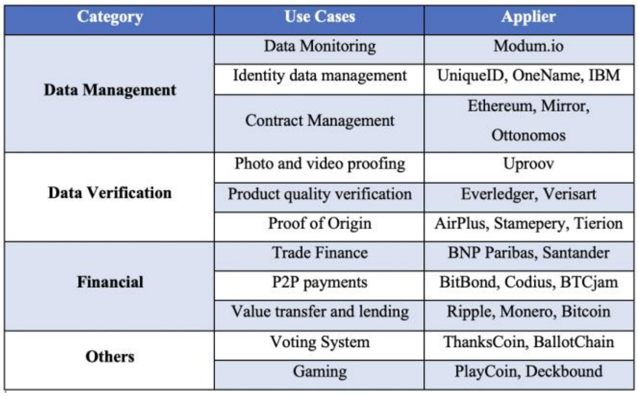
VI. BLOCKCHAIN APPLICATIONS

According to Wang et al (2019), following the success of bitcoin, blockchain was advocated for usage in a variety of implementations and use cases due to its stealthy performance. One of the most popular use cases for Blockchain is in financial services. This technology is used by a number of banks and financial organizations throughout the globe. In addition, Blockchain is still being used for the transmission of cryptocurrency. As a record of ownership, Blockchain may also be employed.

In addition to tangible items like cars, houses, and artwork, it also includes intangibles like digital publications and digital services that can be tracked. For instance, Factom wanted to use Blockchain technology to improve data storage and to enrol in organizations such as enterprises and government agencies. The government sector is another area where blockchain technology is being used (Wang et al, 2019).

Because of the Blockchain's immutability, this technology has been deployed in voting processes across the world. The following table lists a variety of blockchain use cases in several industries, as well as a few companies who have used this technology into their own systems. Nevertheless, as healthcare can be considered as one of the world's most important sectors and the emphasis of this paper, the healthcare use cases will be thoroughly described (Wang et al, 2019) as shown in Table III.

TABLE III. BLOCKCHAIN APPLICATIONS (WANG ET AL,2019)



Category	Use Cases	Applier
Data Management	Data Monitoring	Modum.io
	Identity data management	UniqueID, OneName, IBM
	Contract Management	Ethereum, Mirror, Ottonomos
Data Verification	Photo and video proofing	Uproov
	Product quality verification	Everledger, Verisart
	Proof of Origin	AirPlus, Stamepery, Tierion
Financial	Trade Finance	BNP Paribas, Santander
	P2P payments	BitBond, Codius, BTCjam
	Value transfer and lending	Ripple, Monero, Bitcoin
Others	Voting System	ThanksCoin, BallotChain
	Gaming	PlayCoin, Deckbound

VII. BLOCKCHAIN IN HEALTHCARE

A. *Biomedical Research and Education*

There are several potential applications for Blockchain technology that may be found in pharmaceutical education and research. It is considerable that the need of blockchain for healthcare has increased due to the current covid-19 pandemic too. Blockchain may aid in the elimination of data fabrication and misreporting in clinical studies, as well as the exclusion of unsatisfactory clinical research findings. Due to the anonymization of the encrypted data, blockchain facilitates patients' authorization for the use of their records in clinical studies. Furthermore, the immutability aspect of this technology ensures the integrity of blockchain-collected data for clinical research (Ahmad et al., 2020).

B. *Electronic Medical Records*

One of the most prevalent examples of blockchain's use in the healthcare industry is found in the management of electronic health records. Electronic medical records are responsible for the generation, storage, and preservation of patients’ medical, personal, or health information digitally. According to this use case, decentralization, data provenance and immutability are among the properties that make Blockchain a good fit (Agbo, Mahmoud and Eklund, 2019).

Smart contracts, confidentiality and security are also considered. According to reports, Guardtime is an instance of a firm that employs a blockchain-based network to secure more than 1 million medical data records in Estonia. Another example is the medrec project, that aims to purvey people access to their medical information (Agbo, Mahmoud and Eklund, 2019).

C. *Remote Patient Monitoring*

The method of remote patient monitoring involves the collection of biological data via the use of body area sensors, Internet of Things devices, or mobile devices in order to remotely follow the state of the patient. As previously reported, there are several instances of remote patient monitoring systems that demonstrate how smart contracts may assist a real-time patient tracking program that can give automated therapies in a secure setting (Agbo, Mahmoud and Eklund, 2019).

D. *Pharmaceutical supply chain management system*

As it is mentioned by Haq and Muselemu (2018), one of the other clear use cases for blockchain is in the logistics of the medical and pharmaceutical supply chains. Although the consequences of delivering fake or substandard medications to patients are significant, this is an ongoing issue for some drug manufacturers. To address this problem, blockchain technology was mentioned. The overall objective is to monitor all prescription drug activity on a blockchain network that is connected to all relevant parties. Using this method, anyone who changes or tries to change the prescription on purpose can be caught. This new business venture makes use of blockchain technology to provide immutability by making available to the public temperature data that are used for the management of pharmaceutical supply chains.

VIII. BLOCKCHAIN SECURITY

Using blockchain technology is a new advancement in safe networking that does not need centralized control in a distributed network setting. There are several ways to think about blockchains, but one of the most common is to think about them as distributed databases that store transaction records in a hierarchical order. By using intelligent and decentralized usage of crowd computing cryptography, the blockchain network is developed and kept by a peer-to-peer network (Wang et al., 2019).

When users of the network are wary of each other, blockchain technology provides a decentralized cryptographic database that facilitates trustful transactions. There is no doubt that blockchain technology has seen increased success on a global scale. The ledger of a blockchain network has to keep track of each transaction. Because this database cannot be altered in any way, existing entries cannot have their information changed or deleted (Wang et al., 2019).

Due to the fact that this database is decentralized, it is impossible for anybody to access the transactions or the sensitive data. Block chaining is an important component of the blockchain since each block carries a hash value and is connected to the one before it through the prior block's hash. Due to the fact that changing this parameter would have an effect on the whole chain, the intruder would not be able to alter any block (Wang et al., 2019).

IX. MEDICAL RECORD MANAGEMENT SYSTEMS

A. *The History of Patient Records*

The earliest record that is known to exist was made in Egypt in 1600 B.C., but it was not a real patient record. Instead, it was a written document on papyrus that documented surgical care of battlefield wounds. This piece of papyrus paper is shown in the Fig. 3 (Dalianis, 2018).

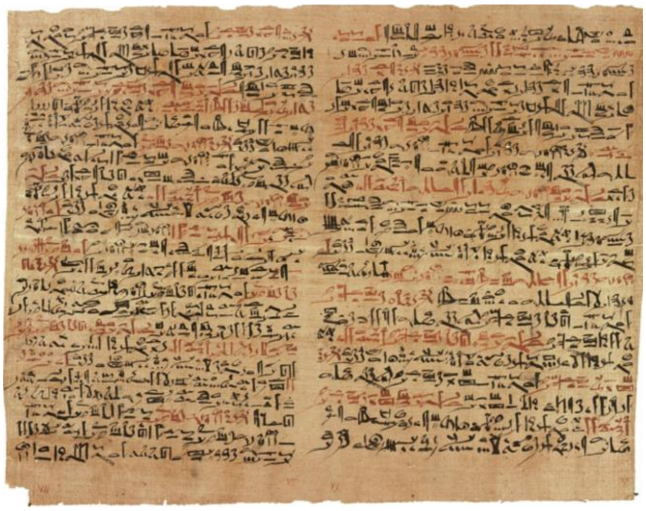


Fig. 3. Edwin Smith Papyrus describing in Egyptian hieratic script (Dailanis, 2018)

Hippocrates, who is frequently referred to as the father of medicine, was active around 2,400 years ago in the temple of healing that was dedicated to the deity Asclepius on the island of Kos, which is located in what is now the eastern part of Greece. Hippocrates believed that medicine should be treated as a science apart from both theology and sorcery. When Hippocrates was deciding how to treat his patients, he made thorough notes regarding the symptoms, look of the patient, social circumstances, and other factors. He also advocated that these papers have to be saved and utilised by future doctors who are engaged in the treatment of the patients (Dalianis, 2018).

Patient records are prepared for a variety of purposes, including serving as a memory aid for the attending physician as well as a resource for use by other doctors who are engaged in the patient's care in some capacity. A variety of clinicians, including nurses, physiotherapists, dietitians, psychologists, etc., contribute to the patient record. There are various names for patient records, including patient record, case history, health record, and case sheet. The patient's name, the nature of the visit, and the patient's past and background are all identifiable details in a paper-based medical record (Dalianis, 2018).

B. *Electronic Health Records (EHRs)*

As a result of recent advancements in technology, the vast majority of medical facilities, including hospitals and clinics, have adopted electronic health record management systems. It is important to note that Electronic Health Information, sometimes known as EHRs, were never intended to be used to handle lifetime medical records that span many organizations (Vora et al., 2018).

As patients move from one healthcare provider to another for different reasons, they always leave behind fragmented data that must be reassembled. Since of this, patients will no longer have simple access to data from the past because primary stewardship often remains with the clinician and not with the patient (Xiao et al., 2021).

In accordance with the HIPAA Privacy Rule, providers have up to sixty days to reply to a petition for amending or deleting an incorrectly created record. Aside from the time delay, record maintenance might be difficult to undertake since patients are hardly prompted and rarely allowed to see their whole record. The fragmented way in which patients interact with records reflects the nature of how these data are administered. Due to financial incentives that promote "health information blocking," patients and providers may encounter substantial barriers when attempting to get and share data (Xiao et al., 2021).

X. Blockchain based Medical Record management

For a long time, people have held the vision that electronic health records (EHRs) need to be kept indistinguishable from both time and location and ought to be able to be accessed whenever and wherever the law permits. When it comes to the initial phase of digitization, it didn't matter whether a health care provider kept their patients' medical information on-premises or in the cloud; rather, the provider had control over the data. There is no significant difference between these EMR systems and the traditional paper-based ones since the administration of medical data is simply transferred from paper folders to hard drives thanks to advancements in information technology (Xiao et al., 2021).

In the second stage, authorized medical professionals and staff members across several health care organizations generate, administer, and consult electronic health records (EHRs), which enables interoperability across various EHR systems. In other words, EHRs may transmit medical information across health care professionals and track a patient's information across numerous health care organisations. Nevertheless, the implementation of such systems is impeded by both technological and legal obstacles. (Xiao et al., 2021).

To begin, the performance of these systems is bad when it comes to the availability of data, the integrity of data, and the retrieval rate when electronic health records are kept using a distributed or institution-centric paradigm. Second, even though health care providers and government organizations insist that these EHRs are HIPAA compliant, individuals are understandably concerned about privacy and data breaches whenever these systems are out of their hands (Xiao et al., 2021).

It is considerable that using the current health record management systems, more than millions of records have been broken yearly and this has been repeated through either verifiable media resources or government agencies. Therefore, there is an urgent need for a secure, reliable and unique electronic health record management system that can be used by all health care providers. Blockchain technology can be considered as one of the best solutions for the current health management systems (Xiao et al., 2021).

The main reason behind using blockchain technology for this kind of technologies is due to the fact that blockchain is a distributed peer-to-peer database that ensures the availability, reaction speed, and integrity of all stored information. As an added bonus, blockchains may help make eHealth's IoT safer. Second, by using blockchain technology, the users' access can be controlled. For accomplishing this task, a smart contract can be regulated which will define the required access control. BHEEM can be considered as an example for blockchain based health record management system (Vora et al., 2018).

As it has been mentioned by Xiao et al. (2021), healthChain can be considered as a real-world example for the electronic health records management system. It is considerable that healthChain works according to a governance paradigm, and it guarantees both the availability of data and the integrity of data. This system offered a chaincode API in order to satisfy the criteria presented by a variety of customers. Proof-of-Authority (PoA) is a consensus algorithm that is used by this system, as has been stated.

The second real-world example of blockchain based health record management system is MedRec. This system solves four primary difficulties, including the sluggish access to medical data, the lack of interoperability across systems, the lack of patient agency, and the scattered access to medical data. MedRec uses a private, peer-to-peer network, and the information included in each block indicates the ownership and access rights for a given set of data. The block content in MedRec symbolizes data ownership and viewing rights shared by members of a private system (Ekblaw et al., 2016).

XI. Conclusion

With the contributions of different cutting-edge technology, healthcare systems are able to govern and keep an eye on the health of their patients. It is essential that the development of these systems have a clear and unambiguous focus on increasing the effectiveness of these systems. One of the main reasons behind the development of efficient healthcare management system is due to the fact that healthcare industry can be considered as one of the most important industries globally.

Blockchain technology can revolutionize the healthcare management system with its numerous benefits including data integrity, transparency and traceability. Electronic health record management systems can use blockchain technology to preserve and manage patient records while making it accessible at anytime and anywhere for the intended entities. Within this paper, the researcher has gone through some articles related to the chosen topic and a literature review has been provided accordingly.

It is considerable that based on the findings, the researcher has gained a lot of information regarding blockchain, its benefits, applications and security. Besides that, the healthcare applications of blockchain are deeply analyzed. It is mentionable that the main focus of this paper was regarding the health record management system.

References

Agbo, C., Mahmoud, Q. and Eklund, J., 2019. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare*, 7(2), p.56. Available at: <https://www.mdpi.com/2227-9032/7/2/56>

Ahmad, R., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S. and Omar, M., 2020. Blockchain and COVID-19 Pandemic: Applications and Challenges. [online] Available at: <http://researchgate.net/profile/Samer_Ellahham2/publication/346170823_Blockchain_and_COVID-19_Pandemic_Applications_and_Challenges/links/5fbca29b458515

b797641bce/Blockchain-and-COVID-19-Pandemic-Applications-and-Challenges.pdf>

Ahmed Farah, N. A. (2018). Blockchain Technology: Classification, Opportunities, and Challenges. *International Research Journal of Engineering and Technology*, *5*(5). https://www.irjet.net/archives/V5/i5/IRJET-V5I5659.pdf

Bashir, I., 2018. Mastering Blockchain - Second Edition. Packt Publishing.

Dalianis, H. (2018). The History of the Patient Record and the Paper Record. *Clinical Text Mining*, 5–12. https://doi.org/10.1007/978-3-319-78503-5_2

Ekblaw, A., Azaria, A., Halamka, J. D., Lippman, A., & Vieira, T. (2016). *A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research*.

Haq, I. and Muselemu, O., 2018. Blockchain Technology in Pharmaceutical Industry to Prevent Counterfeit Drugs. *International Journal of Computer Applications*, [online] 180(25), pp.8-12. Available at: <https://www.researchgate.net/publication/323872197_Blockchain_Technology_in_Pharmaceutical_Industry_to_Prevent_Counterfeit_Drugs>

Keat, L. G., & Keong, L. K. (2021). Blockchain-based academic certificate credentialing system for Asia Pacific University. *Journal of Applied Technology and Innovation*, *5*(3), 20–26.

Khatoon, A., 2020. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics*, 9(1), p.94. Available at: <https://www.researchgate.net/publication/338380336_A_Blockchain-Based_Smart_Contract_System_for_Healthcare_Management>

Lo, C. K., Batcha, N. K., & Mafas, R. (2020). Applying Blockchain Technology to Secure Dataset Used for Data Analytics. *Journal of Applied Technology and Innovation*, *4*(1), 1–5.

Loke, Y. C., Batcha, N. K., Sakinah, N., & Ziz, N. S. B. N. A. (2020). Blockchain-Enabled Election Voting System. *Journal of Applied Technology and Innovation*, *4*(4), 51–55.

Morel, R. J., Keong, L. K., & Kiat, K. G. (2022). E-voting system using blockchain technology. *Journal of Applied Technology and Innovation*, *6*(1), 24–29.

Rathore, H., Mohamed, A., & Guizani, M. (2020). Blockchain applications for healthcare. *Energy Efficiency of Medical Devices and Healthcare Applications*, 153–166. https://doi.org/10.1016/B978-0-12-819045-6.00008-X

Sahu, M., 2021. *Cryptography in Blockchain: Types & Applications [2021] | upGrad blog*. [online] upGrad blog. Available at: https://www.upgrad.com/blog/cryptography-in-blockchain/

Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Member, S., Kumar, N., Obaidat, M. S., of IEEE, F., of SCS, F., P C Rodrigues, J. J., & Abdullah, K. (2018). *BHEEM: A Blockchain-based Framework for Securing Electronic Health Records*. https://doi.org/10.1109/GLOCOMW.2018.8644088

Wang, H. L., Chu, S.-I., Yan, J.-H., Huang, Y.-J., Fang, I.-Y., Pan, S. Y., Lin, W.-C., Hsu, C.-T., Hung, C.-L., Lin, T.-C., & Shen, T.-T. (2020). Blockchain-Based Medical Record Management with Biofeedback Information. *Smart Biofeedback - Perspectives and Applications*.

Wang, H., Wang, Y., Cao, Z., Li, Z. and Xiong, G., 2019. An Overview of Blockchain Security Analysis. *Communications in Computer and Information Science*, Available at: <https://link.springer.com/chapter/10.1007/978-981-13-6621-5_5> https://doi.org/10.5772/INTECHOPEN.94370

Xiao, Y., Xu, B., Jiang, W., & Wu, Y. (2021). The HealthChain Blockchain for Electronic Health Records: Development Study. *Journal of Medical Internet Research*, *23*(1). https://doi.org/10.2196/13556

Yaga, D., Mell, P., Roby, N. and Scarfone, K., 2018. Blockchain technology overview. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf