Journal of Engineering Research

Volume 7 | Issue 3 Article 11

2023

Blockchain for Healthcare Systems: Concepts, Applications, Challenges, and Future Trends

Mostafa Eltabakh, Mohamed nasr, Emad Abdelrahman, Roayat Abdelfatah

Journal of Engineering Research (ERJ)
Vol. 7 – No. 3, 2023
©Tanta University, Faculty of Engineering
ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

Blockchain for Healthcare Systems: Concepts, Applications, Challenges, and Future Trends

Mostafa AbdelwahedEltabakh[1], Mohamed Elsaid nasr[2], Emad Abdel Rahman [3], Roayat Ismail Abdelfatah[4]

[1]Teaching Assistant at Department of Electronics and Electrical Communications Engineering, Faculty of Engineering, Tanta University.
email: mostafa.eltabakh@f-eng.tanta.edu.eg
[2] Department of Electronics and Electrical Communications Engineering, Faculty of Engineering, Tanta University
[3] Department of Electronics and Electrical Communications Engineering, Faculty of Engineering, Tanta University
[4] National Telecommunication Institute.

***Abstract*- Electronic medical records are digital documents that contain medical data pertaining to a patient's medical care. Because electronic health records are regularly exchanged amongst stakeholders in healthcare, they are prone to a range of challenges such as data misuse, loss of privacy, and security. These may be solved via blockchain-based technologies in the healthcare area. That is the decentralized innovative technology to completely transform, reshape, and reinvent how data is stored and processed in healthcare sector. This article offers an overview of blockchain, its formation, types, and how it works. A variety of applications of blockchain in medical field that could revolutionize such an industry are introduced. Previous scientific research on the application of blockchain to Electronic Health Record systems (EHRs) is highlighted. Finally, the open research problems that limit the use of blockchain in the medical field is discussed.**

***Keywords*- Blockchain, EHR, Healthcare, Consensus.**

I. INTRODUCTION

A paper-based system has been used in the medical sector to store patients' data and their medical history with analysis results for many years before modern technological advances. However, this system suffered from security and organizational problems due to the different medical records in all medical institutions visited by patients.

EHRs have mostly supplanted the traditional typescript of patient health records, to decrease healthcare costs, and enhance patient care quality. Reliance on EHRs helps to get rid of problems resulting from fraud and human error. Recent advances in healthcare systems provided doctors with excellent facilities for remotely collecting, analyzing and monitoring healthcare information for patients [1]. A medical server is used to store a digital copy of the medical history of a patient, which includes immunizations, medications, allergies, diagnoses, and treatment plans. Furthermore, doctors frequently want to know a patient's medical history from disparate doctors at assorted hospitals before making a diagnosis or treatment [2]. These modern medical systems aim to upgrade the follow-up of diseases and the causes of their occurrence, the effectiveness of medicines and the strategies for the prevention of chronic diseases.

Despite the advantages of EHRs, there is a danger in using digital systems to transmit such high-sensitivity files and personal information. Any unauthorized access could cause data breaches. A complete EHR file for a single patient can run into hundreds of dollars [3]. Thus, data confidentiality and privacy for both organizations and individuals have become a serious matter that deserves attention. So, a forthcoming solution for sharing data is based on blockchain which allowing coordinated clinical diagnosis in telemedicine accurately[4]. If one key component is hacked, (A single Point of Crash), the entire system will stop working in the centralized security. Such worries can be allayed by blockchain's decentralization without the assistance of a reliable third party. So, blockchains have been thoroughly integrated into a variety of applications that are intimately tied to every element of our everyday lives, such as cryptocurrencies, business, smart cities, IoT, and others, with the help of their decentralized qualities [5].

Blockchain is a database or distributed digital ledger, introduced by Satoshi Nakamoto [6], that stores and records digital transactions and data. All participants can see the same version of the digital ledger and validate each transaction before being stored on the blockchain. This means that data cannot be changed or erased without the awareness and approval of all participants. It is tamper-proof and secure as it uses cryptography to secure and authenticate each transaction that takes place within a blockchain network [7]. Timestamp and cryptographic hash are used in blockchain to make its records immutable once created. So, it is easy to detect any fraudulent attempt to manipulate records [8].

The application of blockchain in the field of healthcare plays a role in preserving the privacy of patient records and makes the exchange of this information between doctors, hospitals, pharmacies, and medical laboratories a transparent and secure process. This means that all medical sector institutions can view the same version of the ledger and trust all the data in this record have been verified before being added, which enhances the confidence of members that existing data is accurate and up to date. Therefore, the use of blockchain preserves the privacy of patient data and lowers the possibility of it being manipulated [9-11]. In addition, due to its decentralized character, its usage helps to reduce the cost of maintaining healthcare data because there is no need for third-party intermediaries.

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (ERJ)
Vol. 7 – No. 3, 2023

ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

This survey paper aims to demonstrate blockchain's impact on securing of electronic health records (EHRs).It sheds light on many blockchain applications in healthcare. It also provides a review of blockchain research related to security solutions for electronic health records. In addition to, it discusses some of the problems and opportunities associated with the application of blockchain-based technology in the field of healthcare. Finally, it addresses the current use of blockchain in electronic health records as well as its future advancements.

After this introduction, section II delves into the blockchain, its types, construction, and how it works. Section III deals with healthcare problems and the role of blockchain in solving it. Section IV presents challenges and opportunities of blockchain-based healthcare systems. Section V covers recent research studies on using blockchain to secure EHRs. Section VI summarizes the open challenges impeding the adoption of blockchain in securing EHRs. Finally, section VIII sums up the article and discusses future research options.

II. BLOCKCHAIN

This section explains the blockchain principle, its architecture, and its various types. It also discusses in some detail the different types of consensus mechanisms.

A. *Blockchain Concept*

Satoshi Nakamoto invented blockchain technology, a Proof of Work "PoW" chain that uses hashes. It serves as a tool for internet-based transactions that do not involve a banking institution. Using digital signatures in the usual coin pattern gives excellent ownership control but is insufficient without a way to prevent double-spending. To address this, a peer-to-peer network that retains a public record of transactions was created that makes it computationally hard for hackers to modify [6].

A blockchain can be thought of as a data structure that facilitates peer-to-peer value exchange via transactions without the requirement for a central, dependable adjudicator. It is a "distributed ledger", which means that each member within the network has an electronic copy of the whole ledger, which is disseminated throughout the network among all peers. This ledger is "cryptographically secure," indicating that security functions that make it safe against modification and misuse have been provided through cryptography. Some of these services include data integrity, source authentication, and non-repudiation. Blockchain is append-only, which means that data can only be inserted into the chain in time-sequential order. This makes it virtually hard to modify data that has already been uploaded to blockchain, thereby rendering it immutable. In other words, blocks that are added to the chain cannot be modified, making it a tamper-proof and immutable record of transactions. However, it might be altered in exceptional circumstances where malicious actors collude to seize more than 51% of the power on the blockchain network. Otherwise, it is essentially unchangeable [12].

The most important feature of a blockchain is that it can only be updated through consensus. There is no centralized authority responsible for maintaining the ledger. In contrast, each update is evaluated against severe criteria defined by blockchain protocol and is added to the chain only once all participating nodes on the network establish consensus. Many consensus algorithms guarantee that participants firmly agree on the validity of the final state of the data within blockchain network.

Blockchain uses distributed ledgers to store records of all transactions that occur. When a transaction occurs among two peers on blockchain, it is recorded and appended to a block. Each transaction has an immutable hash signature. Because of this hash and the distribution among all nodes in the chain, an unauthorized alteration in the blocks would be seen and ignored, making it nearly difficult to tamper with data throughout the blockchain. Fig. 1 depicts the way each block is linked together, and Fig. 2 depicts how hash signatures during transactions function. They offer together an immutable system.

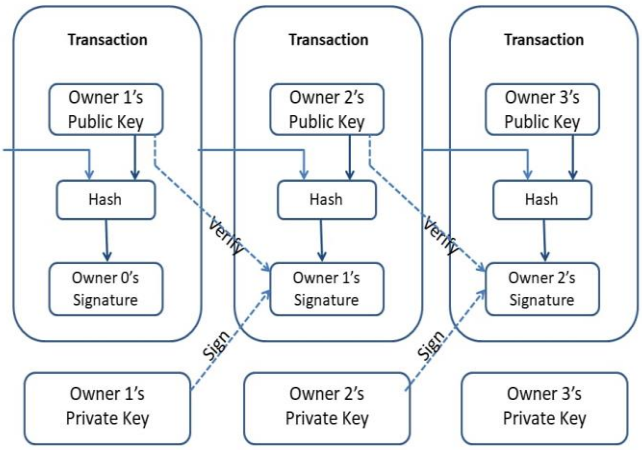

Figure 1. Hash signing, as demonstrated in [6].

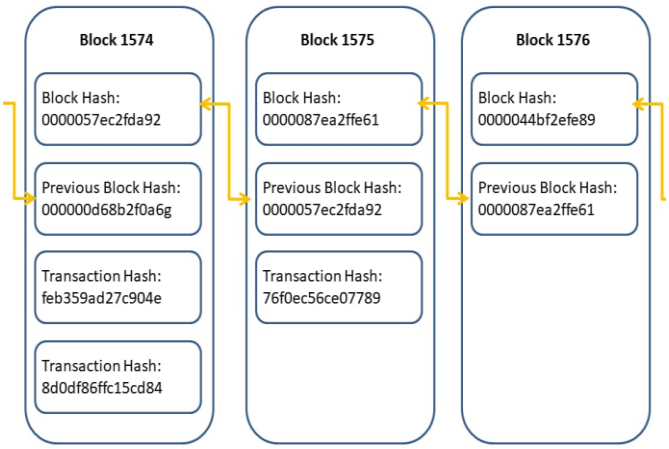

Figure 2. Block linking as illustrated in [13].

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (ERJ)
Vol. 7 – No. 3, 2023
©Tanta University, Faculty of Engineering
ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

B. *Blockchain Construction*

Transactions that occur within a period are documented in a file known as a block, which serves as the foundation of the distributed ledger network.

A blockchain is a block-by-block chain as shown in Fig.3. Each block contains a particular number of verified transactions along with other critical information. All blocks are encrypted and connected in a linear fashion, by recording the hash of the previous blocks. Preceding block hash is used to calculate current block hash. Genesis block is the first without a prior block hash.

Figure 3. Blockchain structure.

Blocks can be thought of as data structures in the blockchain database that permanently record transaction data. A block contains either some or all the latest transactions that have not yet been confirmed by the network. It is closed once the data has been confirmed. Then, a new block is established to accept and validate new transactions. Thus, a block is the permanent storage of records that, once recorded, cannot be changed or removed.

As seen in Fig. 4, a block serves as a data storage unit that holds a large amount of information [14], but it only takes up a little space on your computer [15].

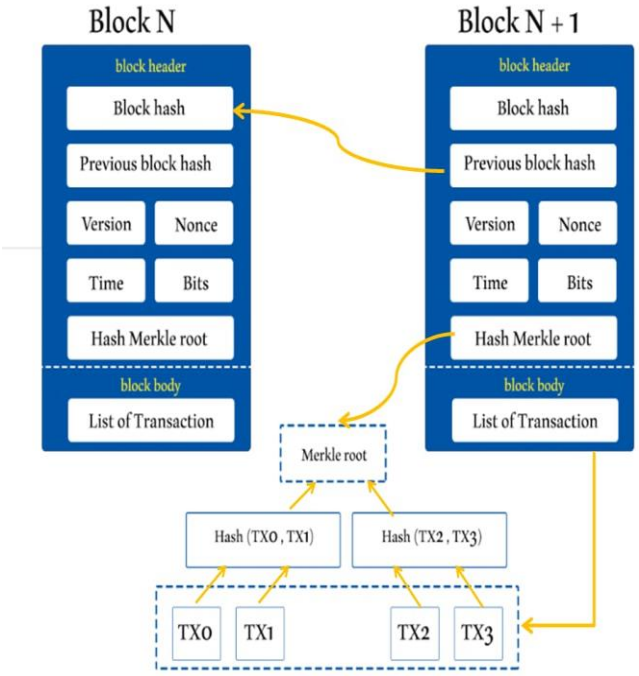

Figure 4. Block structure.

The block header comprises an 80-byte field containing metadata about the block. It is used for identifying a certain block within the blockchain. It manages all blockchain blocks. Miners change the nonce value to hash a block header regularly as part of typical mining operations [16]. Let's take a brief look at the six elements of the block header. These elements are commonly seen in blocks, but they may differ depending on the type [14]:

- **Version:** The digital currency version that is currently in use.
- **Previous block hash:** An encrypted hash of the prior block's header. It comprises a 32-byte field that contains a 256-bit hash (generated by SHA-256) that identifies the preceding block. This assists in the construction of a blockchain.
- **Time**: A timestamp for inserting the block into the blockchain. It is the digitally recorded time at which the block was mined. It validates transactions.
- **Nonce:** An encrypted code that a miner has to solve to validate and close the block. It is the only changeable element in a block. PoW miners alter the nonce till they get the proper block hash.
- **Bits:** It is a 4-byte parameter that indicates the complexity of adding the block. It's sometimes referred to as "difficulty bits" Which indicates how tough it is to solve the nonce. The block hash must be smaller than the difficulty level, according to PoW.
- **Hash Merkle root:** It is a 32-byte field that contains a 256-bit hash. It is constructed hierarchically by combining hashes of each transaction in the block, as seen in Fig. 5. A Merkle tree keeps track of all transactions in each block by establishing a unique digital fingerprint for each one. It enables users to

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (ERJ)
Vol. 7 – No. 3, 2023

ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

determine whether or not a transaction is eligible to be listed in a block [12].

Each transaction in a Merkle tree is hashed, then each pair of transactions is combined and hashed together until there is only one hash for the entire block. If the number of transactions is odd, one of them is doubled and its hash is combined with itself.

When viewed from above, this building resembles a tree. In Fig. 5, "T" represents a transaction, and "H" represents a hash. It is important to note that the figure is oversimplified, an average block has more than 500 transactions, not eight.

The hashes that are in the bottom row are referred to as "leaves,", those in the center as "branches,", and the one at the top as the "root.". The header contains the Merkle root of a particular block. To generate the block's unique hash, the root is merged with additional information (the software version, the preceding block's hash, the date, the difficulty goal, and the nonce) and then passed through a hash function. This hash is unique from the Merkle root because it is not included in the relevant block but in the next one.

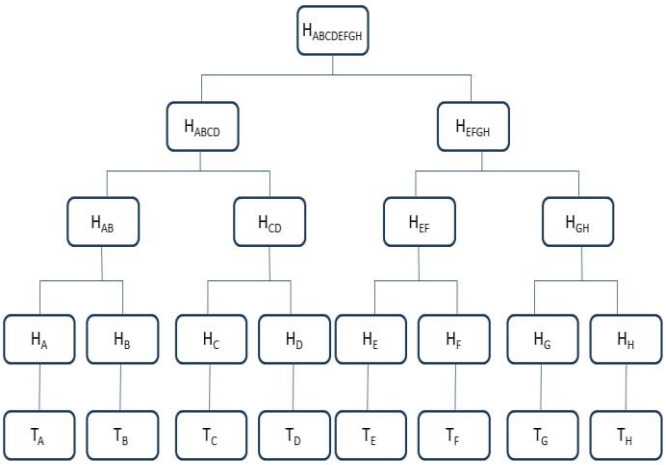

Figure 5. Merkle tree.

The block's body includes publicly verifiable transactions.

It's a variable-length field that holds all transactions within the block. The size and number of transactions within a blockchain block fluctuate. It is determined by the level of network congestion and communication overhead.

C. Blockchain Types

There are presently three different kinds of blockchain systems, in consortium, private, and public networks. To grasp the distinction in between, it is critical to acknowledge that the open nature of technology varies greatly depending on its underlying architecture. It can be designed in various ways, such as permissionless or permissioned blockchain. Everyone in the network can observe all transactions in a permissionless blockchain, and anybody can become a participating node in the system if they want by consuming CPU cycles and providing PoW. However, blockchains can also be constructed to be permissioned, allowing for tighter control over the chain because participation in the network requires permission, limiting the individuals who may engage on the chain. After distinguishing between permissionless and permissioned blockchains, it is now possible to delve into the three previously described forms of blockchain networks shown in Fig. 6.

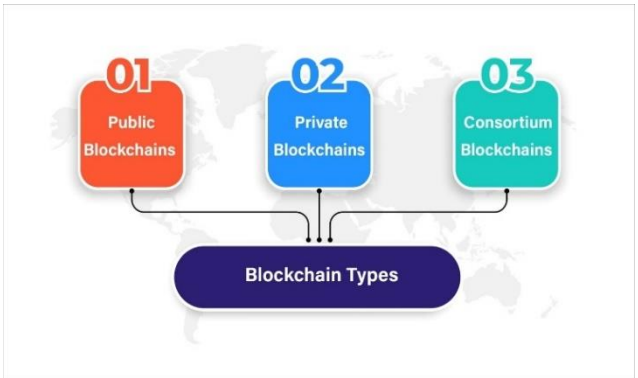

Figure 6. Blockchain types.

1. **Private Blockchain:** Is best defined as one that operates in a closed environment. It also serves as a permissioned blockchain which is controlled by an entity. Participants must consent to be part of the network, making it an exclusive network. Transactions in this network are private and available only to individuals who have granted consent to join the network. Hyperledger and Corda are excellent examples of such networks.
2. **Public Blockchain:** It is a prominent sort of Blockchain that is open and decentralized. In this form, computer networks are available to everyone interested in transacting. The person gets the transaction rewards depending on validation, where two types of Proof-of-stake (PoS) and PoW models are utilized. It is also a distributed and non-restrictive ledger system that does not require any form of authorization, and anyone with access can be authorized to obtain data or parts of the blockchain. It also provides authority for current and historical record verification. This is also used for cryptocurrency mining and exchange. The most common blockchains in this sector are Bitcoin, Litecoin, and Ethereum. It's highly secure if stringent security rules and practices are followed. However, failing to observe security protocols might be dangerous [17].
3. **Consortium Blockchains:** They are permissioned and somewhat decentralized, with a pre-selected number of nodes regulating the mechanism used for consensus. These nodes frequently take the shape of a small group of like-minded institutions. This implies that

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (ERJ)
Vol. 7 – No. 3, 2023
©Tanta University, Faculty of Engineering
ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

participating nodes often have proven identities, as interaction involves some invitation.

D. Consensus Mechanisms

When data propagation by nodes over a blockchain network begins, no centralized body is responsible for controlling and solving disputes or protecting against intrusions. As a result, a means to trace the movement of funds and ensure an indisputable financial exchange is required to prevent fraud, such as double-spending [16]. For this ledger to retain a consistent state, all nodes must agree to a common content update mechanism, and blocks should not be accepted to be a part of the blockchain without the majority's permission. This is referred to as a consensus technique, and it entails the construction of blocks, which are subsequently included in the existing ledger for future usage. There are several types of consensus methods. However, the most frequent blockchain consensus mechanisms are summarized in Fig. 7 [12, 17-20].

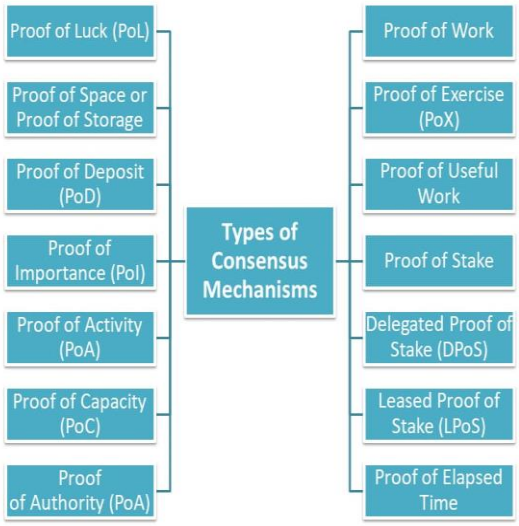

Figure 7. Types of consensus mechanisms.

1. **Proof of Work:** It is the initially developed and most extensively utilized mechanism as in Ethereum and Bitcoin. Each miner is competing to solve the same mathematical challenge; once solved, the process restarts. PoW challenge is a mathematical puzzle, and the reward is provided to the first miner who successfully solves the challenge. The validated transactions are then recorded in the public ledger. The greater the number of miners in the network, the more complex the computational challenge must be solved. Miners are rewarded with cryptocurrency when they solve a problem. The name originates from the prize representing proof of work done.

   PoW has numerous drawbacks. For example, blockchain security is jeopardized if a single mining pool holds over 51 percent of the overall mining power due to a centralized collective, equivalent to having a single computer. So, a DOS attack on a network may have an impact on the network's overall reliability [16].

2. **Proof of Stake:** PoS is influenced by the number of coins a node holds. The node has to stake the exact number of coins it wants to mine. PoS makes use of stake power rather than hashing power. Therefore, there's no dependency on energy consumption since there is no challenge to solve. PoS employs an algorithm based on block hashing similar to PoW used in Bitcoin, except that the number of peers is limited. This provides the required security while simultaneously minimizing the cost and power consumption. A network fee is collected instead of rewarding peers for completing a mathematical task, as in PoW.

   The amount of the peer's stake determines which peer executes the work in PoS. This provides distributed consensus while using less energy and spending less on cost. Any peer may participate in the mining process by staking currency to validate a new transaction. You may become a miner in two ways: stake your currency to be utilized by an authentic node or just propose a complete node to be chosen to serve as a miner. Because most currencies are controlled by a few miners, decentralization is limited.

   Each miner is chosen at random for the work; It has no dependence on solving a challenge [16].

3. **Delegated Proof of Stake:** DPoS tries to address PoS difficulties by replacing the random mechanism of picking a miner with democracy. By dividing the mining process into two sections, DPoS creates technical democracy.

   - Election: While electing an assembly of block producers, there are only 21 available, as opposed to infinite in PoW.
   - Production scheduling: Each of the 21 block producers takes turns producing a block every 3 seconds.

   The person holding the wallet can vote for the validator to create a new block. Rather than competing like in PoS and PoW, validators can be merged to form a new block. This encourages improved opportunities for reward distribution by voting for a regular delegate, who in turn will distribute incentives back to them, resulting in decentralization. The voters must check the validator's honesty to guarantee a stake [16, 18].

4. **Proof of Exercise (PoX):** It is a conceptual consensus process built for distributed ledgers that requires a large portion of the system's computational resources. To reduce resource waste, an attempt is being undertaken to convert the hash-based PoW puzzle-mining process to a beneficial outcome. As an exercise, a form of PoW solves real-world computational issues by examining matrices. DNA-RNA matching, data mining, and image processing are matrix-based real-world scientific problems [18].

5. **Proof of Useful Work:** This idea was presented to address scientific problems utilizing orthogonal vectors as proof of work, and it also incorporates the zero-knowledge proof

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (ERJ)
Vol. 7 – No. 3, 2023

ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

concept. As a result, the miners can only submit proof of the solution, not the solution itself, to the delegated assignment. Only after a specific pre-set condition in the network is met does the solution become available [18].

6. **Leased Proof of Stake (LPoS):** It is the least popular PoS variation, focusing on 'the rich become richer' problem. It encourages participants to lease the stake to vote for the node, and the new block is formed by the node with the most stake. The obtained prize will then be allocated to all leasing participants. The mechanism also encourages the number of leasing competitors to earn rewards, hence increasing the protocol's security. This technology is ideal for creating a public transaction platform. It is safer and more efficient for building public cryptocurrencies [18].
7. **Proof of Elapsed Time:** PoET employs a Trusted Execution Environment which offers safety and randomization in the leader selection procedure through the use of a guaranteed wait time [12].
8. **Proof of Luck (PoL):** This protocol instructs each round's participants to commit all uncommitted transactions to a new block, and the version block is given a numerical value. Following that, the voting procedure begins, in which participants vote on a number at random, and the node with the most votes gets the luckiest block. Shortly after the luckiest block is received, the remaining network participants stop mining and their block is broadcasted, reducing network congestion [18].
9. **Proof of Space or Proof of Storage:** It is a protocol designed to prevent resource abuse, comparable to proof of work. However, instead of computing, it requires disc usage. Proof of space is intended for publicly distributed ledgers, and free disc storage is regarded as a resource. The effect of a miner's power over the network is directly proportionate to the quantity of disc space donated [21, 22].
10. **Proof of Deposit (PoD):** Nodes who want to join the network have to pay a security deposit before they can begin mining and submitting blocks[12].
11. **Proof of Importance (PoI):** This concept is significant and distinct from PoS. It is based not just on how much of a stake an individual has in the system, but also on how the user uses and moves tokens to build confidence and importance. It is utilized in the blockchain of the NEM coin [12].
12. **Proof of Activity:** This technique combines PoS and PoW to ensure that a stakeholder is chosen in a pseudorandom yet uniform manner. When compared to PoW, this is a more energy-efficient technique. It employs a novel idea known as "Follow the Satoshi". PoW and PoS are coupled in this technique to reach a consensus and a high level of security. This system is more energy efficient since PoW is only utilized in the first step of the mechanism; after that, PoS is employed, which consumes little energy [12].
13. **Proof of Authority (PoA):** Participants in this situation are not expected to solve arbitrarily complex mathematical problems, as in PoW, but rather to employ a pre-configured collection of "authorities" allowed to collaborate trustlessly. Particularly, some nodes are only permitted to secure the blockchain and create new blocks. PoA systems are often appropriate for consortium private networks in which some preselected real authorities are permitted to control the material that is published to the public registry. Those nodes will be given a set of private keys to use to sign new blocks as trustworthy signers [23].

III. Blockchain Technology in Healthcare

Blockchain has the ability to completely reshape the healthcare sector as a whole. Vast amounts of data are created, accessed, and stored in the medical field daily. The healthcare industry must be able to access, change, and rely on data created by diverse activities inside the healthcare organization. For patients' privacy and data interchange, specific properties such as interoperability, provenance, access control, information sharing, and data integrity must be observed. These characteristics are required for establishing confidence between the data proprietor and the servers who store it in the health care system. The ability to effortlessly interact and exchange information across diverse parties is referred to as interoperability. The goal is to improve individual and population health. The documented record of past events is known as data provenance. It prevents data manipulation by making all data collected, processed, and accessed by researchers auditable and transparent.

Real-world data is in high demand from many research institutes. Any unauthorized information exchange or misuse of private information gradually erodes the public's confidence in healthcare.

To address the aforementioned issues, an alternative strategy must be considered. Because of characteristics such as decentralization and data integrity, blockchain could be a better choice. It could also increase data integrity, interoperability, provenance, access control, and information sharing across various parties. As a result, blockchain technology could serve as an entirely novel infrastructure that helps to build confidence in the healthcare business. [24]. Following are some blockchain applications in healthcare:

A. Settlement of a Health Insurance Claim

Health insurance is provided to provide care and to safeguard an individual's assets against loss caused by disease treatment, accidents, or medical emergencies. Depending on the type of insurance acquired, it may cover medical bills, doctor visits, and surgical expenses. As soon as the insurance companies receive the claim, they undertake a thorough review. A little error, such as a misspelled patient's name, can cause a claim to be rejected. Many claims are denied as the insurer did not receive them, and occasionally the proof to claim is insufficient and the information provided is deficient.

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (JER)
Vol. 7 – No. 3, 2023
©Tanta University, Faculty of Engineering
ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

Smart contracts based on blockchain technology can help to automate settlement procedures by making claims visible to the supplier and insurer. As a result, potential errors and scams are exposed. Another benefit of smart contracts lies in how they ensure that all involved parties are kept up to date when rules or regulations change [25].

The amount of data created in the medical industry is continuously increasing. The fundamental issue of numerous organizations is to safeguard the privacy and security of data from malicious users. Blockchain technology enables data access to various healthcare data users based on credentials assigned to them.

One of the most popular uses of blockchain in healthcare is managing patient records. A patient's medical data is usually shared between different locations, healthcare centers, and insurance providers. All patient records should be combined into an automated procedure to obtain the entire patient's accurate medical history. This may be performed by storing a patient's medical data on a blockchain, which always preserves modernized tamper-proof, and traceable records, such as prescription history, symptom data, facilities obtained, treatment strategy, and payment information [26]. This allows medical practitioners to supply patients with treatments that are timely, efficient, and suitable.

Healthcare professionals can get a comprehensive look at their patient's medical history information clearly and transparently by using blockchain technology. All data is transparent, immutable, secure, and traceable [27].

B. *Patient Digital Identity*

Patient identity matching is an important aspect of health information sharing since it facilitates the retrieval of patient information from a healthcare database. Despite increased development efforts, matching patient data is extremely difficult. Mismatched patient identities can result in erroneous medical data. To alleviate patient matching issues, a system for managing identities that can integrate the patient-identifying techniques utilized by various healthcare providers is required.

Blockchain technology includes a unified decentralized identity system. Cryptographically secure addresses can be used to represent patient identities. The addresses are assigned a unique key, which may verify address ownership without revealing private data about the patient [28].

C. *Data Sharing Among Different Stakeholders*

Before prescribing a medicine for accurate treatment in certain health-related emergency circumstances, a complete understanding of a patient's medical background is essential. For example, a patient with a severe illness may have traveled outside of the nation and may need an emergency consultation with a doctor. This physician would often seek a patient's past medical information in certain scenarios in order to provide better and higher quality healthcare services [29].

A patient's medical history may assist medical professionals in analyzing multiple factors such as medication allergies and prior treatment records, which may lead to the creation of more effective treatment regimens [30].

Sharing medical information across stakeholders such as clinics and hospitals, in addition to research development organizations, and insurance companies may enhance the performance of healthcare providers.

Before sharing information, many hurdles must be addressed. The first concern is data security since it is kept in the public cloud, which has data exposure risks. The second concern is that patients may only have limited access to their health records. Therefore, they need assistance in sharing their knowledge with unfamiliar individuals. The third difficulty is that current systems' centralized design needs trust in the noncentral authority.

Blockchain technology has the ability to greatly enhance information-sharing infrastructure in terms of user-centric access control, privacy, and security [31].

D. *Electronic Health Records (EHR)*

The transformation of paper-based records to HER is one of the most significant advances in modern healthcare delivery. EHRs are patient data storage mechanisms used by healthcare professionals to store data such as medical notes and laboratory test results. They eliminated the problems associated with traditional records. Thus, improved the patient safety by reducing errors and making information more accessible. EHR systems are used in a variety of institutions throughout the world to provide services such as patient appointment management, medical data storage, lab tests, and billing and accounts. EHR system's goal is to provide sharable and secure patient records via several platforms. In spite of being the most often used method of storing patient data, this system has drawbacks such as data breaches, information asymmetry, and interoperability [32]. Personal health records (PHR) based on blockchain are patient-centric apps that enable individuals to access and manage their data. Patients may utilize blockchain-based PHRs to monitor how their health data is shared and used, check the authenticity of their health information, and repair errors in their records.

IV. Blockchain Opportunities in Healthcare

By offering substantial benefits that can be summed up as follows, blockchain technology has the potential to help streamline hospital data management procedures.

A. *Precision medicine and clinical trials*

Clinical trial results may become more reliable via blockchain technology. The problem of publishing erroneous clinical trial data is resolved by maintaining data integrity. This improves the accessibility and accuracy of data analyses that may be performed on clinical trial data. Utilizing blockchain for clinical trial research can assist in addressing several significant challenges, including patient recruiting,

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (ERJ)
Vol. 7 – No. 3, 2023

ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

monitoring, and tracking the clinical supply chain, regaining the integrity of trial data, and shortening the total trial duration. Blockchain technology may be applied to the field of precision healthcare to handle genetic sequences, assisting in the proactive treatment of a wide range of diseases brought on by genetic disorders. According to reports, 10% of chronic illnesses that affect adults are inherited genetically. Genomic sequencing is needed to understand people's DNA profiles, which can treat such diseases. However, obstacles like DNA data intro-permitting and organizations' desire to exchange such information with one another prevent this from happening. The storage of DNA data on a blockchain can provide people the ownership and control over their data [33]. Due to their significant hacker vulnerability, centralized databases which belong to third parties are no longer needed. Because blockchain networks record data securely, anyone is able to share it with anybody for medical research and medication development.

B. Telehealth systems protection

Telehealth systems can break down geographical limitations in healthcare, yet they are subject to cybersecurity threats. If the virtual connection built between the patient and physician is hacked, sensitive information about the patient, such as routine information flows and home activities, might be compromised. For telehealth systems to be successful, security and privacy issues must be resolved. Blockchain technology may help telehealth services to provide security, privacy protection, and trust. It may help to provide a seamless exchange of information, eliminating the need for an intermediary, and increasing client trust in telehealth services. Doctors can now maintain comprehensive patient histories, treatments, and results from laboratories in a decentralized, traceable and immutable way [34].

C. Improving health insurance coverage

Most insurance companies already maintain their data in centralized systems. It takes a long time to share information between stakeholders across the insurance companies. There are many defects in today's health insurance systems. Because all transactions are decentralized, immutable, traceable, tamper-proof, and securely stored on a blockchain, it provides an unprecedented degree of transparency. So, blockchain may be able to solve the interoperability issue. Smart contracts enable the automatic collection of agreement records and transactions, which can enhance administrative procedures. They can also be used to identify fabricated or overstated claims for insurance [35]. Another benefit of blockchain-based technology is that it increases the transparency of patient insurance information for physicians. Via consensus mechanisms, it could help to ease the medical insurance procedure and improve provider directory accuracy. As a result, the idea of using blockchain in the health insurance business is quite beneficial.

D. Consistent preservation permissions

Healthcare providers need quick access to patient information during medical emergencies. Inconsistent permissions may cause a patient's data access to be banned in an emergency, putting the patient's life in peril. Blockchain technology may offer two potential solutions for simple and secure permission management. With the use of blockchain-based smart contracts, access may be granted depending on specified norms agreed upon by all parties involved in the contract [25]. These agreements can be altered to automate various operations. Patients can control access thanks to cryptographic keys. Each patient has a master key that is used in the unlocking of medical information. The patient can grant hospitals or physicians access to their copies if required. Smart contracts may also be used to provide write and read access privileges. Cryptographic keys and smart contacts built on the blockchain can help to reduce mistakes that previously occurred as a result of human error. Blockchain also speeds up the process of collecting patient data.

E. Improved medication traceability

Drug fraud has become a big problem in the field of healthcare. When the medicine manufacturing process is finished, it must be transferred from the production stocks to the distributors, who then transport it to the retailers, which sell it to clients. In this cycle of the supply chain, there is always a possibility that fake medications will enter [36, 37]. The phony pharmaceutical business is estimated to be worth $200 billion each year. In accordance with the organization that funds health research, 10% to 30% of medications supplied globally are counterfeit, [38]. These statistics show how highly susceptible pharmaceutical companies are to fake medications. The drug's manufacturing process may be tracked with the aid of blockchain technology. Blockchain-based transactions are timestamped and unchangeable, ensuring that the data cannot be altered [39]. Public or private blockchain systems can be used by the pharmaceutical industry depending on their operational requirements. The whole drug trial may be obtained via blockchain-enabled technology. When a medicine is moved from one area to another, the movement data may be stored on the blockchain, boosting medicine traceability and decreasing the probability of counterfeit pharmaceuticals being made available to consumers.

F. Medical care billing systems

In past decades, conventional patient billing procedures have sometimes fallen prey to different scams. Furthermore, the current billing system requires more time and resources to compile billing data. The complicated coding employed in the healthcare billing system is one of the leading causes of inadvertent billing mistakes, such as repeated procedures or incorrect files. Medical billing procedures may be improved using blockchain technology and automated coding approaches. Compared to traditional billing methods, blockchain-based technology has the potential to significantly

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (ERJ)
Vol. 7 – No. 3, 2023

ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

simplify and secure the process of payment. When insurance claims were involved, previous payment techniques made it far more difficult to pay the expenditures. These constraints may be lifted by utilizing blockchain to maintain all data immutable, enabling insurance organizations to resolve claims more swiftly while consuming fewer resources, money, and time[25].

V. STATE-OF-ART

The authors in [2] proposed a secure, blockchain-based EHRs sharing system that uses conditional proxy re-encryption and asymmetric searchable encryption to guarantee access control, privacy, and data security. The authors demonstrated their proposed protocol's computational efficiency and superiority over previous corresponding attempts in the field notably when it comes to data security, access control, and privacy. They researched the use of consortium and private blockchains for storing encrypted EHRs and discussed the benefits and drawbacks of each method. To ensure the system's availability in consortium blockchains, they adopted proof of permission as the method of consensus. They simulated fundamental cryptography and deployed their protocol on the platform of Ethereum. There are no constraints mentioned directly in the study. The paper did not address the obstacle of compatibility across different blockchain-based EHR systems, which may be a barrier to wider adoption and integration with existing healthcare systems.

In [40], authors suggested a system based on blockchain technology for managing and securing patients' EHR. The system was built using Ethereum network, Solidity, and web3.js. The proposed system enables decentralized storage while providing security and privacy aspects for patient data and allows for the safe transfer of patient medical records. It incorporates MetaMask, a cryptocurrency wallet, with a centrally controlled, private system that authorities can quickly access and secure. Overall, the study emphasized the ability of blockchain technology to address concerns with EHRs in the healthcare industry and proposed a novel protocol that is both quick and secure to implement. As indicated in the study, future work might include integrating the payment module into the existing architecture via a private blockchain. This may be accomplished via the use of a decentralized structure powered by blockchain technology, whereby a patient pays for a physician's visit using a credit or debit card. The national identity number might be included in the event of verification.

In [28] some examples of blockchain applications in healthcare areas were mentioned such as:

- Detecting drug overdoses by tracking prescriptions.
- The management of every patient's electronic identity so that it corresponds to patient's history.
- Medical insurance claims automation to detect errors and fraud attempts.
- Creating a completely accessible and controlled medical record.
- Data sharing with the healthcare provider to allow the patient to determine which data is authorized.

The paper also investigates the difficulties of implementing blockchain in health care, including privacy protection and system evolution. It proposes healthchain which is a blockchain-based health data privacy solution. Medical diagnoses can no longer be removed or manipulated by implementing healthchain. Patients can use healthchain to download IoT data and obtain comments from doctors. Physicians can view data and comment on it. Data is encrypted and saved on healthchain to minimize computational overhead and preserve privacy. Users can cancel physicians' access at any moment by transferring updated transactions to healthchain.

In [41], authors recommended a blockchain-based consortium model for secure storage and exchange of healthcare information. To establish access controls for the consortium blockchain's encrypted health data, a hybrid storage mode, and an attribute-based access control technique were implemented. Authors conducted substantial research to demonstrate that their suggested approach is both secure and efficient. Finally, they established a Quorum consortium blockchain and deployed smart contracts to simulate transactions on Tencent cloud. The research indicates that, in view of the fast spread of devices and IoT, the security of medical information exchange in human domain networks may be investigated further in future.

Table 1. Summery of the Blockchain-Based Healthcare Systems

Ref	Consensus Mechanism	Blockchain Type	Contribution
[2]	Proof of Permission	Consortium Blockchain	• (EHRs) sharing system via consortium blockchain was proposed. • Ensured privacy and security via asymmetric searchable encryption and conditional proxy re-encryption. • Compared to similar schemes, the proposed protocol offers more security features and demonstrates greater resistance to the Key Generation Algorithm (KGA) issue.

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (ERJ)
Vol. 7 – No. 3, 2023

ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

[40]	Proof of Stake (PoS)	Ethereum	• A blockchain-based system for managing and securing EHRs was proposed. • The proposed system enabled users to obtain the same data simultaneously, which enhanced efficiency and credibility. • In terms of average latency, the proposed system proved its superiority over other techniques.
[41]	Improved Byzantine Fault Tolerance (IBFT)	Quorum Consortium Blockchain	• A secure and privacy-preserving medical data sharing scheme based on consortium blockchain was proposed. • A hybrid data storage pattern was adopted to reduce storage load of blockchain. • The proposed system allowed patients to track the access history of their EHRs. • Enhanced encryption key management via a tree structure used for each patient's EHRs to enable recovery of keys.

VI. OPEN CHALLENGES

This section discusses the most important obstacles to the use of blockchain in securing EHR which can be summarized as follows:

1. Interoperability

It refers to a system's capability to seamlessly interface with another system in order to exchange critical information. The ease with which medical records can be transferred from one service provider to another is referred to as interoperability in an electronic medical record system.

EHR must feature core interoperability to guarantee that the whole system is capable of transmitting and receiving data from other systems. Received data will be instantly accessible in the system. This represents the simplest level of interoperability, enabling just basic data transfer.

EHRs must support structural interoperability, To allow data to flow correctly through the system and allow physicians to see unaltered patient data, EHRs must support structural interoperability. This healthcare data intermediate domain guarantees that patient information is delivered and received in a suitable and shareable way in order to establish a new EHR database utilizing structured messages.

Also, EHRs must have semantic interoperability, which enables data to be accurately reorganized and codified in such a way that any system can receive and comprehend the new information. That is, the language used by one EHR system must be understood by other systems, which is the maximum degree of interoperability conceivable [42].

2. Ensuring accuracy of medical information

The immutability of blockchain technology is an essential aspect. Therefore, ensuring the accuracy of healthcare data transferred to blockchain is crucial. Most existing healthcare data records contain erroneous information for a variety of reasons, including insurance market rivalry, administrative and human errors, and tax avoidance [43]. Consequently, healthcare data records must be updated before being stored on blockchain.

3. Integrating blockchain technology with current healthcare systems

Certain obstacles must be overcome before blockchain can be widely adopted. Among these issues, integrating blockchain with current infrastructure. Healthcare providers must redesign their present systems in order to migrate to a blockchain system. Yet, it's very difficult since it needs a substantial amount of time, careful planning, funding, and human skills to work within current systems to support the seamless transfer of blockchain technology in the medical field. In some situations, reconciliation of blockchain with healthcare systems may be impossible. In such cases, businesses must buy new compatible systems, which incurs extra expenditures.

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (ERJ)
Vol. 7 – No. 3, 2023

ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

4. Scalability

One of the greatest impediments to the broad usage of public blockchains in healthcare is scalability [44]. Traditional transaction networks can handle thousands of transactions every second. In terms of transaction speeds, the Ethereum blockchain lags far behind, with just roughly 20 transactions per second. Scalability does not pose a problem while utilizing private blockchains since processing nodes operate under trustworthy parties [45].

VII. Conclusion and Future Trends

In this article, the need to use EHRs, because of their advantages in eliminating human errors, is investigated. The security problems resulting from unauthorized access to those records, which allows manipulating patient records, and this endangers the patient's health and violates his privacy is also reviewed. Then the role of the block in these problems is discussed. A complete and extensive explanation of the working principle, consensus mechanisms, and types of blockchain have been provided. Then being went through the integration of healthcare systems with blockchain in great depth. We discussed how blockchain can be used in healthcare to handle health data in a transparent, decentralized, auditable, traceable, accessible, reliable, and secure way. Furthermore, blockchain ensures that health data is stored immutably and not tampered with. Follow that a spoke about the benefits of implementing blockchain in healthcare industry. New research studies that demonstrated the usefulness of blockchain in boosting medical sector health services is discussed. Also, the open research problems that are impeding the widespread use of blockchain technology in the medical field have been discussed. Blockchain is expected to revolutionize the medical field by enhancing data security and operational efficiency. Nevertheless, there are significant technological hurdles to integrating healthcare systems with blockchain, such as complexity, interoperability, the difficulty of integrating with existing healthcare systems, and scalability. Those must be addressed in future research studies.

There are many open research points in this innovative theme as follows:

a) Big Data

When big data is available, it could be used to leverage all healthcare data to advance prediction areas in healthcare diagnosis. Acquiring and processing massive amounts of personal medical data, especially from wearable devices and mobile, while avoiding privacy breaches, is a key challenge for healthcare systems. By enabling traceability, immutability, and security, blockchain technology can overcome the security problems concerned with big data approaches.

b) Internet of Medical Things (IoMT)

IoMT refers to a group of applications and medical equipment that communicate with healthcare information technology systems via computer networks connected to the Internet. Wi-Fi-enabled medical devices provide machine-to-machine connectivity that is the foundation of IoMT. By utilizing wearable devices and IoMT, medical service providers can get updated, real-time health information for patients even if they are in remote locations. As a result, the patient's medical information recorded on blockchain will always be up to date [46].

c) ARTIFICIAL INTELLIGENCE (AI)

Integrating blockchain and AI in various health applications can make them more stable and efficient. A variety of machine learning techniques can be used to identify fake EHR data, ensuring that only genuine EHRs are stored on blockchain. Future diseases can also be precisely predicted using deep learning with EHRs stored in blockchain [47].

Funding: No funding has been provided for this research.

Conflicts of Interest: The authors undertake to have no conflicts of interest.

References

[1] K. Chaudhary, U. Kant, and P. Kumar, "A View on the Blockchain as a Solution to the Healthcare Industry: Challenges and Opportunities," in International Conference on Computational Intelligence, Security and Internet of Things, 2019: Springer, pp. 160-169.
[2] M. Alsayegh, T. Moulahi, A. Alabdulatif, and P. Lorenz, "Towards Secure Searchable Electronic Health Records Using Consortium Blockchain," Network, vol. 2, no. 2, pp. 239-256, 2022.
[3] M. Chernyshev, S. Zeadally, and Z. Baig, "Healthcare data breaches: Implications for digital forensic readiness," Journal of medical systems, vol. 43, no. 1, pp. 1-12, 2019.
[4] E. C. Cheng, Y. Le, J. Zhou, and Y. Lu, "Healthcare services across China–on implementing an extensible universally unique patient identifier system," International Journal of Healthcare Management, vol. 11, no. 3, pp. 210-216, 2018.
[5] H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo, "A survey of state-of-the-art on blockchains: Theories, modelings, and tools," ACM Computing Surveys (CSUR), vol. 54, no. 2, pp. 1-42, 2021.
[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, p. 21260, 2008.
[7] F. C. Maldonado, Introduction to Blockchain and Ethereum: Use distributed ledgers to validate digital transactions in a decentralized and trustless manner. Packt Publishing, 2018.
[8] J. Norton, "Blockchain easiest ultimate guide to understand blockchain," ed: CreateSpace Independent Publishing Platform, 2016.
[9] B. Shen, J. Guo, and Y. Yang, "MedChain: Efficient Healthcare Data Sharing via Blockchain," Applied Sciences, vol. 9, no. 6, p. 1207, 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/6/1207.
[10] M. Kassab, J. DeFranco, T. Malas, P. Laplante, G. Destefanis, and V. V. G. Neto, "Exploring research in blockchain for healthcare and a roadmap for the future," IEEE Transactions on Emerging Topics in Computing, vol. 9, no. 4, pp. 1835-1852, 2019.
[11] S. Idrees, M. Nowostawski, and R. Jameel, "Blockchain-Based Digital Contact Tracing Apps for COVID-19 Pandemic Management: Issues, Challenges, Solutions, and Future Directions," JMIR Medical Informatics, vol. 9, no. 2, pp. e25245-e25245, 2021.
[12] I. Bashir, Mastering Blockchain: A deep dive into distributed ledgers, consensus protocols, smart contracts, DApps, cryptocurrencies, Ethereum, and more. Packt Publishing Ltd, 2020.
[13] M. Gupta, "Blockchain For Dummies 3rd IBM Limited Edition, America," ed: John Wiley & Sons, Inc, 2020.

Doi: 10.21608/ERJENG.2023.227863.1207

Journal of Engineering Research (ERJENG)
Vol. 7 – No. 3, 2023

ISSN: 2356-9441 https://erjeng.journals.ekb.eg/ e ISSN: 2735-4873

[14] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," Journal of network and computer applications, vol. 126, pp. 45-58, 2019.
[15] Y.-C. Liang and Y.-C. Liang, "Blockchain for dynamic spectrum management," Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence, pp. 121-146, 2020.
[16] E. Elrom, The Blockchain developer: A practical guide for designing, implementing, publishing, testing, and securing distributed Blockchain-based projects. Apress, 2019.
[17] P. Tasca and C. J. Tessone, "Taxonomy of blockchain technologies. Principles of identification and classification," arXiv preprint arXiv:1708.04872, 2017.
[18] P. Raj, K. Saini, and C. Surianarayanan, Blockchain technology and applications. CRC Press, 2020.
[19] W. Wang et al., "A survey on consensus mechanisms and mining strategy management in blockchain networks," Ieee Access, vol. 7, pp. 22328-22370, 2019.
[20] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," IEEE Access, vol. 9, pp. 43620-43652, 2021.
[21] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "Proofs of space," in Annual Cryptology Conference, 2015: Springer, pp. 585-605.
[22] L. Lu, K. Yuanyuan, and Y. Yong, "A Novel Approach for Improving Accuracy for Distributed Storage Networks," in International Forum on Financial Mathematics and Financial Technology, 2021: Springer Nature Singapore Singapore, pp. 65-80.
[23] P. Tasca and C. J. Tessone, "A taxonomy of blockchain technologies: principles of identification and classification. Ledger 4 (2019)," arXiv preprint ArXiv:1708.04872, 2019.
[24] S. M. Idrees, M. Nowostawski, and R. Jameel, "Blockchain-based digital contact tracing apps for COVID-19 pandemic management: Issues, challenges, solutions, and future directions," JMIR medical informatics, vol. 9, no. 2, p. e25245, 2021.
[25] M. A. Bazel, F. Mohammed, and M. Ahmed, "Blockchain technology in healthcare big data management: Benefits, applications and challenges," in 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA), 2021: IEEE, pp. 1-8.
[26] S. Wang et al., "Blockchain-powered parallel healthcare systems based on the ACP approach," IEEE Transactions on Computational Social Systems, vol. 5, no. 4, pp. 942-950, 2018.
[27] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: a systematic review," in Healthcare, 2019, vol. 7, no. 2: MDPI, p. 56.
[28] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, "Blockchain technology use cases in healthcare," in Advances in computers, vol. 111: Elsevier, 2018, pp. 1-41.
[29] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain utilization in healthcare: Key requirements and challenges," in 2018 IEEE 20th International conference on e-health networking, applications and services (Healthcom), 2018: IEEE, pp. 1-7.
[30] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE access, vol. 5, pp. 14757-14767, 2017.
[31] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," Journal of medical systems, vol. 42, pp. 1-11, 2018.
[32] A. Shahnaz, U. Qamar, and A. Khalid, "Using blockchain for electronic health records," IEEE access, vol. 7, pp. 147782-147795, 2019.
[33] I. A. Omar, R. Jayaraman, K. Salah, and M. C. E. Simsekler, "Exploiting ethereum smart contracts for clinical trial management," in 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), 2019: IEEE, pp. 1-6.
[34] R. W. Ahmad, K. Salah, R. Jayaraman, I. Yaqoob, S. Ellahham, and M. Omar, "The role of blockchain technology in telehealth and telemedicine," International journal of medical informatics, vol. 148, p. 104399, 2021.
[35] D. Park and D. Ryu, "Blockchain in health insurance: sharing medical information and preventing insurance fraud," Korean Journal of Financial Studies, vol. 48, no. 4, pp. 417-447, 2019.
[36] S. Tendulkar, A. Rodrigues, K. Patel, and H. Dalvi, "System to fight counterfeit drugs," in Advanced Computing Technologies and Applications: Proceedings of 2nd International Conference on Advanced Computing Technologies and Applications—ICACTA 2020, 2020: Springer, pp. 465-470.
[37] P. Pandey and R. Litoriya, "Securing e-health networks from counterfeit medicine penetration using blockchain," Wireless Personal Communications, vol. 117, pp. 7-25, 2021.
[38] M. Sahoo, S. S. Singhar, and S. S. Sahoo, "A blockchain based model to eliminate drug counterfeiting," in Machine Learning and Information Processing: Proceedings of ICMLIP 2019, 2020: Springer, pp. 213-222.
[39] R. Kumar and R. Tripathi, "Traceability of counterfeit medicine supply chain through Blockchain," in 2019 11th international conference on communication systems & networks (COMSNETS), 2019: IEEE, pp. 568-570.
[40] F. K. Nishi et al., "Electronic healthcare data record security using blockchain and smart contract," Journal of Sensors, vol. 2022, pp. 1-22, 2022.
[41] D. Zhang, S. Wang, Y. Zhang, Q. Zhang, and Y. Zhang, "A secure and privacy-preserving medical data sharing via consortium blockchain," Security and Communication Networks, vol. 2022, 2022.
[42] A. Haddad, M. H. Habaebi, M. R. Islam, N. F. Hasbullah, and S. A. Zabidi, "Systematic review on ai-blockchain based e-healthcare records management systems," IEEE Access, 2022.
[43] M. Graglia, C. Mellon, and E. Akin, "Prerequisites for Incorporating Blockchain into a Registry," Last visited, vol. 1, 2020.
[44] A. A. Mazlan, S. M. Daud, S. M. Sam, H. Abas, S. Z. A. Rasid, and M. F. Yusof, "Scalability challenges in healthcare blockchain system—a systematic review," IEEE access, vol. 8, pp. 23663-23673, 2020.
[45] C. R. De Meijer, "Remaining challenges of blockchain adoption and possible solutions," online, accessed, vol. 5, no. 11, p. 2021, 2020.
[46] F. Girardi, G. De Gennaro, L. Colizzi, and N. Convertini, "Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain," Electronics, vol. 9, no. 6, p. 884, 2020.
[47] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, "Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications," IEEE transactions on network science and engineering, vol. 8, no. 2, pp. 1242-1255, 2019.

Doi: 10.21608/ERJENG.2023.227863.1207