SJIF Impact Factor: 6.711

WORLD JOURNAL OF ADVANCE HEALTHCARE RESEARCH

ISSN: 2457-0400
Volume: 8.
Issue: 6
Page N. 215-240
Year: 2024

Original Article www.wjahr.com

EXPLORING THE USE OF BLOCKCHAIN TECHNOLOGY INHEALTHCARE SYSTEMS: CURRENT RESEARCH ON USE CASES, CHALLENGES, AND POTENTIAL FUTURE DIRECTIONS

***[1]Oriolowo Temitope, [2]Folasade Agbolade, [3]Chioma Obi, [4]Kehinde Falayi, [5]Moyosoluwa Ogunyemi and [6]Oluwatoyin Ogunyemi**

[1]Department of Public Health Glasgow Caledonian University Scotland, UK.
[2]Department of Computer ScienceTowson University Towson, USA.
[3]Department of Health Science Towson University Towson, USA.
[4]Department of Health Science Obafemi Awolowo Univerity Ile-Ife, Nigeria.
[5]School of Law Indiana University-Purdue University Indiana, USA.
[6]Department of Computer Science University of Bristol Bristol, UK.

Article Received date: 23 March 2024 **Article Revised date:** 13 May 2024 **Article Accepted date:** 03 June 2024

***Corresponding Author: Oriolowo Temitope**

Department of Public Health Glasgow Caledonian University Scotland, UK.

ABSTRACT

Transparency, auditability, trustworthiness, privacy, and security are some of the issues plaguing existing healthcare data management systems. Other concerns include data origin tracing, immutability, traceability, and auditability. In addition, many of the healthcare data management systems in use today are centralized, which increases the risk of a single point of failure and makes them susceptible to natural disasters. The emerging decentralized technology known as blockchain has the potential to completely revamp, transform, and change the way healthcare organizations handle patient data. This article offers a comprehensive overview of blockchain architecture, platforms, and classifications to assist in the selection of the most suitable blockchain platform for healthcare applications. This compilationpresents the latest discoveries from state-of-the-art research on healthcare blockchain and current healthcare applications that are based on blockchain technology. Furthermore, to provide insight into future research, we present the challenges and prospective areas of study. We utilized threat model classifications to analyze the various security attacks on the blockchain protocol and conducted a comparative analysis of detection and prevention techniques. In addition, this paper also covers techniques to enhance the privacy and security of the blockchain network.

KEYWORDS: Healthcare management, Blockchain, Internet of Things, Health care insurance.

I. INTRODUCTION

Fast developments in the IoT paradigm have revolutionized healthcare organizations by bringing about substantial im- provements to electronic health records (EHRs), prescription drug databases, and insurance data.[46] Medical devices that are connected to the internet can collect important patient data, improve workflows, provide useful information about symptoms and patterns in sickness, enable remote care, and give patients more choice over their lives and treatments.[93] Patients can be monitored in real-time with the help of IoT devices. There will be less need for frequent trips to the doctor's office as a result of their use. Reduced hospital visit duration and readmission costs are two benefits of intercon- nected home health monitoring systems. By sounding alarms and sending out messages before a potentially life-threatening disease develops, medical devices connected to the internet of things (IoT) can assist with diagnosis. Attached sensors to various parts of a patient's medical equipment can gather data and send it to the hospital, where a doctor can check it forany abnormalities.

The healthcare business has unquestionably benefited from the continual innovations brought about by the Internet of Things (IoT).[47] The widespread use of electronic health records (EHR) and electronic medical records (EMR) has made secure management of this data a significantly more challenging task.[48] The growing frequency of cybersecurity assaults has rendered most existing healthcare systems vulner- able due to their centralization, which can lead to data breachesand single

points of failure.[13] Serious consequences may result from the unlawful disclosure of patients' private and sensitive information. In addition, when it comes to EHR and EMR, current medical systems aren't up to the task of providing transparency, trustworthy traceability, immutability, auditing, privacy, and security.[35] Blockchain technology has the potential to solve the problems that current healthcare systems are experiencing[4] An estimated 100–150 billion in yearly savings might be achieved by 2025 through the use of blockchain technology. Costs related with data breaches would go down, and fraudulent activities and counterfeit goods would go down as well, leading to these savings.[89]

One area where blockchain shows a lot of promise is in healthcare data management, where it might substantially enhance operational efficiency. It does this by guaranteeing trust between all parties and providing data efficiency that is unmatched.[92] Data access flexibility, interconnectedness, security, transparency, immutability, authentication, and decen- tralized storage are just a few of the remarkable and inherent properties provided by the technology. All of these features make blockchain technology ideal for healthcare data man- agement.[2] By using smart contracts, blockchain technology removes the need for middlemen by establishing terms and conditions that are agreed upon by all healthcare participants in the network.[39] It reduces administrative costs that aren't necessary. Public key cryptography, consensus mechanisms, and peer-to-peer networks are the three main tenets around which blockchain is built.[36] Based on how permissions are managed, blockchains can be classified as either public, private, or consortium blockchains.[14] Public blockchains allow every user with an Internet connection to take part in reaching consensus. By utilizing proof-of-work or proof- of-stake procedures, public blockchains integrate incentives and secure digital verification. Due to the anonymity of its users, the public blockchain system is completely open and accessible to everybody interested. When just one business owns the network, we say that it's a private blockchain. Based on this, reaching consensus using this blockchain type requires a trustworthy third party. Combining public and private blockchains, the consortium blockchain maximizes their respective strengths. If your group's goal is to improve internal communication, then this is the perfect tool for you. Since every blockchain network has its own set of pros and cons, healthcare companies are free to select the one that best suits their needs and use cases. The use of blockchain technology in healthcare has been the subject of numerous surveys in the past.[85] The scope and substance of our poll set it apart from theirs. Further, unlike other polls, this one covers a wide range of important features of blockchain technology, such as its inherent characteristics, new prospects, and potential challenges. Blockchain technology's function in healthcare data management is explored in this article. Here are the main things that we have accomplished.

- We provide comprehensive examinations of the essential attributes of blockchain technology, along with its notablebenefits in the healthcare industry.
- We Offered clarification on blockchain's operational paradigm, architecture, and categorization.
- We assess and discuss the main opportunities offered by blockchain technology in the healthcare sector.
- We examine several case studies to illustrate the practi- cality of incorporating blockchain technology into healthcare systems.
- Provided a comprehensive examination of different blockchain security threats and a comparative review of currenthealthcare blockchain applications.
- We scrutinize and discuss important unresolved research challenges, and propose some prospective recommendations.

The contributions are provided in different sections, specif- ically sections 2 to 9. The last thoughts and future proposals can be found in Section 10.

II. OVERVIEW OF BLOCKCHAIN

Although its 2008 introduction by Satoshi Nakamoto to the financial industry was its initial use case, blockchain technology has since evolved into a foundational technology for numerous decentralized applications.[39] Cryptography and decentralized, peer-to-peer networks come together in blockchain technology. The cryptographic hash functions con-nect the several chunks that make it up. The blockchain is an easy-to-understand but very ingenious way to automate and protect the transfer of data. To initiate a transaction, one of the parties involved must first construct a block. This block is being confirmed by thousands of machines spread out over the internet. A unique record with a distinct history is created when the verified block is added to a chain and kept throughout the internet. Therefore, in blockchain, contracts ensure that transactions are legitimate when the consensus of blocks agrees. Because blockchain technology is decentralized, users must have faith in one another to share keys, which is crucial to the system's functionality.

Blockchain technology has come a long way in its short lifetime. From version 1.0 to version 5.0, we catalog five distinct blockchain implementations. When it comes to de- centralized ledgers that can record transactions and store data across multiple computers, the most fundamental is blockchain1.0, the version that Nakamoto released. Simple English: early blockchains could only record the monetary worth of a"athing" that changed hands periodically. Digital currencies likeBitcoin, Ripple, and others used to be the" thing" we were talk-ing about. Vitalik Buterin's planned upgraded cryptocurrency, Blockchain 2.0, is sometimes called the rise of Ethereum (2014). Ethereum was the first blockchain to incorporate a smart contract technology. Smart contracts, in their simplest form, are collections of scripts that, when certain conditions are satisfied, automatically execute

various actions. Businessesand individuals can engage in more complex transactions than simple cryptocurrency trades through these agreements. Decentralized autonomous groups and decentralized distri- bution apps are good fits for it. Distributed applications, such as enterprise blockchain, are more broadly applicable to blockchain 3.0. Blockchain 3.0 has several potential uses, including in the healthcare industry, cybersecurity, manufactur- ing, and supply chain management. Industry 4.0 and healthcare 4.0 are both supported by the evolving blockchain. Improving the industry's user experience is its primary goal. Some examples of blockchain 4.0 systems are Rchain and Metaverse. The fifth generation of blockchain technology is currentlyunder development. The goal is to make the blockchain more secure and less prone to its usual downsides. Blockchain 5.0 has several potential uses, including Hashgraph, Hedra, and Relictum pro.

A. State of the Art of Blockchains in Healthcare

Concerns specific to the healthcare sector include authen- tication, non-repudiation, mobility, access control, security, and interoperability. The needs of the healthcare sector are graphically depicted in Fig. 1 Files, wearable sensors, and

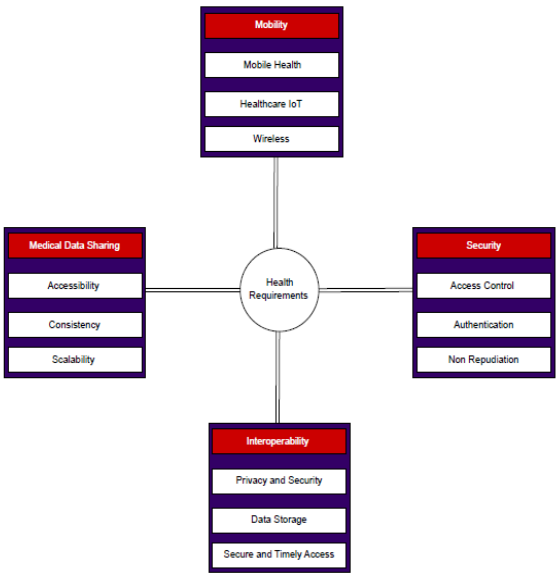

Fig. 1: Industry requirements for healthcare.

other apps are gathering healthcare data in the age of Industry 4.0. Electronic Health Records (EHR), Electronic Medical Records (EMR), and Personal Health Records (PHR) are the three main formats for the digital health data. Ensuring proper authentication is in place to control access to such data isvital. Healthcare data retrieval queries should also be checked with suitable access control to prevent manipulation threats.[65] Encryption is also inefficient when it comes to protecting medical documents.[91] note that interoperability concerns may arise if various encryption algorithms are used to secure different kinds of health records. According to Andrew et al. (2021)[10] numerous privacy issues might arise as a result of inadequate security measures for healthcare data. Additionally, healthcare data must be interoperable. According to Gohan et al. (2022)[33], interoperability refers to the capacity to share and transmit data across many sources. Centralized data storage is the foundation of interoperability.

When it comes to healthcare data, centralizing storage poses challenges such as slow access, security risks, and privacy concerns. Since healthcare data tends to grow in size over time, it would be impractical to send it all via untrusted channels to a central repository. The centralized nature of the data also makes it difficult to have secure and timely access to it. Consistency, accessibility, and scalability must beensured during data exchange in the medical field to facilitate the many different types of medical research that rely on it.[1] Because patients increasingly demand their data to be portable, mobility is becoming an increasingly important requirement in the healthcare business. The proliferation of internet-connected smart devices, sensors, and other devices makes data transfer capabilities paramount. Some of the many types of mobility include wireless, healthcare IoT, and mobile health. Wireless body area networks (WBANs), sensors, and cellphones are all part of mobile health. Securing data sharing, building trust, controlling access, and managing user consent are all obstacles in mobile health. Problems with network availability, adaptability, responsibility, data integrity, etc., alsoaffect WBAN's wearable body sensors. Another area that offers mobility in the healthcare sector is healthcare IoT. The benefits to both patients and clinicians from healthcare IoT are substantial. On a variety of health issues, patients can be accessed and monitored remotely. But there are a lot of privacy and security issues with data collecting and sharing.[35]

B. User Requirements of Healthcare Blockchain

Privacy worries, technological issues, and the absence ofa mechanism for determining the appropriate use or sharing of data all contribute to the current state of non-cooperation among healthcare organizations. Patients and other healthcare organizations do not always have instantaneous access to their health records. Fig. 2 shows and describes the most prevalent and significant user requirements for blockchain- based healthcare systems that can alleviate possible challenges.

1) Performance: The speed, agility, and efficiency of healthcare systems built on the blockchain are significantly enhanced by the integration and streamlining of numerous operations.[69] Because of its adaptability and ease of use, it enhances the efficiency and effectiveness of healthcare facili- ties in treating patients. Management of outpatient departments (OPDs), inpatient departments (IPDs), and diagnostics; reac- tion to emergencies; invoicing and payment processing; and operations are among the many duties that have been tailored to the platform's characteristics. Users can be granted role- based control in the system, which allows

them to access one or more functions. This helps with monitoring and recording all activities needed for healthcare service.

2) Interoperability: Many issues, including patient involve-ment, privacy, security, and governance, arise as a result of the shift towards patient-centered interoperability. By creating a trustworthy method of data exchange, blockchain technology presents a tempting answer to these problems.[62] In con- clusion, blockchain offers a thorough framework for secure communication between a patient and several parties, letting the patient prove their identity across various institutions and permanently storing their health records.

3) Realibity: If other systems are affected by technical out- ages, disturbances, or malfunctions, the blockchain-powered healthcare system will be able to withstand them with ease.[92] The system has a very secure data architecture and an intuitive yet complicated user interface, making it easy tooperate. There isn't a huge lot of time required for the upgrading process, and the maintenance tasks can be scheduled to correspond with low demand periods. Regular routine tasks are not disrupted by remote updates and improvements to the medical records. For the system to work, the resources and system must be available at all times.

4) Access control: A doctor must get a patient's permission before they can view their medical records. Failure to follow the doctor's instructions will result in the system refusing access. The same holds true for doctors: if a patient wants a regular access privilege, the doctor should ask them directly. In order to comply, the patient must provide his permission before anyone can view his medical records. The patient can independently issue or revoke access credentials for other users of the system and provide temporary access.

5) Security: The healthcare system must monitor the cre- ation, sharing, storage, and analysis of massive amounts of data at all times during the hospital's operations. By leveragingcutting-edge digital technology, the system safeguards all data transfers to the cloud, preventing any possibility of data loss or unwanted access. Every time, the platform meets or exceeds a country's most demanding standards for data security and privacy. Moving the hospital's data to remote servers in the cloud keeps it safe from cybercriminals. Overarchingly, a healthcare system that utilizes blockchain technology fosters openness, safeguards information, stops data theft, and makes hospitals run smoothly. If two healthcare organizations set up a blockchain network, they can use Hyperledger to exchange data across a decentralized database, doing away with therequirement for users to trust each other.[28] Additionally, it makes the exchange of medical transactions quick, safe, and transparent.

6) Healthcare records: Private information about patients' diagnoses, treatments, and outcomes from surgeries is stored in medical records. Paper records are still used for archiving in traditional healthcare organizations. Dispersed among several organizations and areas, electronic health records are presentlyin a state of disarray. There isn't a centralized mechanism to update and distribute these records in real time, even while healthcare supply chains are becoming more digital. This situation has the potential to become far more problematicdue to concerns about the privacy and confidentiality of patient data. Utilizing devices that are Internet of Things enabled allows for the immediate generation of medical data. New developments in blockchain technology, often called distributed ledger technology, provide solutions to problems with data accessibility and data sharing. Patients can gain agency over their healthcare with the use of personalized digital health records since they provide patients with secure, individualized access to their medical records.[22] With the use of PHRs, a new platform can be built that combines digital treatments, smart contracts, and medical data retrieval and storage. The main goal of the system is to establish trustworthy mechanisms of consent for data sharing among various institutions and applications, and to empower patients to use their data to improve their medical care. The adoption of blockchain-based solutions in personalized healthcare records requires the integration of event-driven smart contracts, health record data, and a patient monitoring and control system.

III. BLOCKCHAIN IMPORTANCE IN HEALTHCARE

A. Traceability

According to Martinez et al. (2023), traceability allows forthe permanent monitoring of transactions across the network.

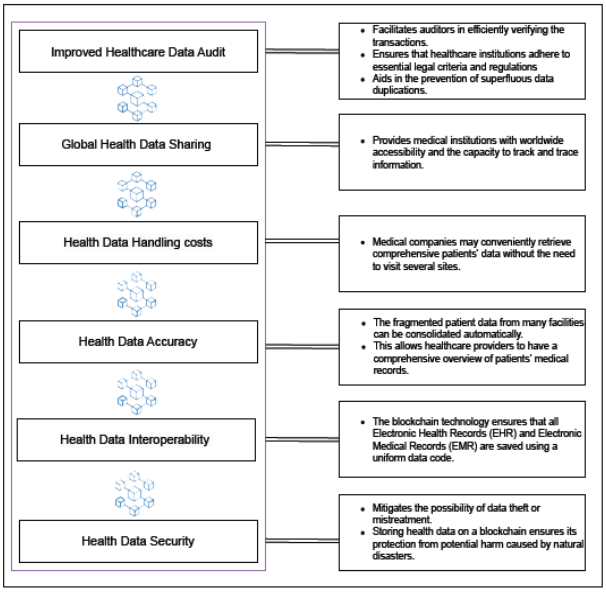

Fig. 2: Blockchain Importance for Healthcare.

.[60] Because everyone can see what's happening, pinpoint when things are happening, and find out who agrees on how to execute the deal are all simple tasks. This feature guarantees that all participants act honestly and take responsibility for their actions. The tremendous interest in blockchain technol- ogy in the past several

years has led to several businesses offering solutions for traceability that are made possible by this technology. Nevertheless, the data quality that was gathered and transmitted has not been improved by these techniques. Therefore, and understandably, there is a great deal of skep- ticism about blockchain's utility in supply chain contexts. Incorporating additional transactions inside a block ensures that they are immutable and have a timestamp. This ensures the data saved in the block remains intact and makes data tracking easier. Organizations that record data or transactions on the blockchain must be highly trustworthy to ensure traceability and validity.

A complicated network is formed by the many different companies that make up the healthcare supply chain. This includes patients, pharmacies, manufacturers, distributors, rawmaterial suppliers, and hospitals. Several reasons, including a lack of data, overly centralised administration, and inconsistent actions from stakeholders, contribute to the difficulties of monitoring shipments along this network. A number of nations have passed legislation requiring all pharmaceuticals to be traceable in some way.[61] Because it ensures the product's authenticity and attempts to track the product's chain of custody along the supply chain, medication traceability has become an essential part of the pharmaceutical supply chain.

B. Data exchange

Blockchain technology ensures data transfer security with- out relying on a central authority or third party. According to Radanovic et.al(2018)[67], blockchain uses a decentralized consensus-based access mechanism to guarantee consistency and reliability. By using public-key cryptography, blockchain technology prevents counterfeiting by guaranteeing the secu- rity and integrity of transactions. Digital signatures may be accessed by authorized users thanks to the identity network security system, which also helps to prevent fraud and data theft.[12] The trustworthiness, compliance with rules, security, auditability, and value of the data sent are all crucial for its success. Blockchain technology provides a number of viable options for facilitating trustworthy, verifiable, and efficient datatransfer within a data ecosystem. Data is guaranteed to remain open, confidential, compatible, and protected by blockchain technology, which also ensures its integrity, traceability, and consistency.

Medical records and other healthcare services can be ac- cessed in a decentralized, transparent, scalable, and secure manner with the DASS-CARE architecture proposed by Ay- ache et al. (2022)[13] using Blockchain technology. With this framework in place, real-time data access and modification might be substantially simplified without sacrificing the safety, privacy, or integrity of patients' information. The hospital's private blockchain system was proposed by Liu et al. (2019b)[53] as a means of securely transferring and preserving pa- tients' medical records. Decentralization, transparency, and tamper resistance are just a few of the security requirements that this system meets. Medical records can be safely stored and accessed by doctors via an encrypted system that places an emphasis on patient privacy.[73] Individuals' symptoms can also be compared using a symptom-matching technique. When people with the same symptoms sign up, they can confirm one other's identities and generate a session key to use for future health-related conversations.

C. Transparency

There is a really interesting feature of blockchain tech- nology. Every single transaction can be seen by anybody who wants to look.[83] Consequently, the security of thedata is ensured. Because they go through digital verification once everyone agrees, they can't be hacked. There can be no deletion or manipulation of data without the explicit consent of all participants, since all changes require their unanimous ac- ceptance. However, there are obstacles to overcome while im- plementing transparency. Blockchain technology's enormous energy consumption and astronomical costs might make its adoption difficult. In addition, the ledger's integrity could be jeopardized if validating smart contracts and transaction veri- fication becomes an unfeasible pursuit. According to Raddatz et al. (2018)[68], it is important to make sure that blockchain users are aware of the rules regarding changes. After the infrastructure that uses this ledger is built, a number of issues will be fixed. There is a lack of documentation for the softwareor firmware code since there is no mandatory requirement to describe this infrastructure. It is crucial to take all of these factors into account while building the infrastructure that will allow democratic environments to use blockchain technology and promote transparency.

Electronic health records, or EHRs, are the current standard for patient data storage in hospitals. However, there has alwaysbeen a problem with trust and openness between organi- zations. By supplying an immutable record with restricted data accessibility, the blockchain can alleviate this problem. Data collection is permanent and data stays accessible for on-demand verification at any time. How well all links in a supply chain understand and can access product-related information is what we mean when we talk about transparency. A blockchain traceability solution that affects the transparencyof various supply chain distribution network designs was introduced in the study by Sunny et al. (2020).[80] The study also emphasizes the ways in which smart contracts and the Internet of Things (IoT) help to expand blockchain's potential,as mentioned by Zhang et al. (2018).[99]

D. Immutability

Politou et.al (2019)[66] highlight that immutability is a significant aspect of blockchain. A blockchain's immutability ensures that the ledger cannot be updated or altered in any way, making the blockchain a permanent

and unchangeable record. The distributed and decentralized nature of blockchains, where consensus is reached among nodes that own the duplicated data, must be understood. This agreement guarantees that the uniqueness of the data will be preserved. There needs to be third-party verification that centralized databases are secure because they are vulnerable to hacking and security breaches. According to Fanning Centers (2016)[30], blockchain technol- ogy records every transaction in a decentralized database. Eachparticipant in the blockchain receives a copy of the distributed ledger. Any transaction that is added to the blockchain cannot be altered once it is there. The use of hash keys allows for the recording of all transactions in blocks. There is a connection between the blocks that come before and after the hash keys. The transactions are validated by each block using the same algorithm. Consequently, other blocks in the network are able to identify any changes made to the transaction because each alteration produces a unique hash key. Blockchain technology ensures that its ledgers remain permanently updated. The distributed ledgers synchronize with each other in real-time as they are spread out throughout all the nodes. Considering the large number of participants, acquiring 51% network control is necessary to manipulate the ledgers.[17]

IV. THE BLOCKCHAIN'S OPERATIONAL MODEL

There is hope that blockchain technology can improve tradefinance services. Blockchain is a system that uses a crypto- graphic peer-to-peer networking mechanism that is distributed and decentralized. A safe environment for digital currency is provided by it. Businesses, communities, and economies standto benefit greatly from implementing blockchain technology. Security, maximum performance, scalability, and effective consensus methods are some of the real-time application needs that blockchain technology encounters in its many uses. Blockchain technology offers an alternative method ofconducting financial transactions directly with the beneficiary. In addition to offering a high degree of security against illegal access or manipulation, the blockchain guarantees the ability to trace and validate the user's money. The principle behind the blockchain is to make it easier to trade goods andservices without relying on third parties or a trusted third party. Implementing transparent transactions can eliminate this issue. Digital data is stored in the blocks that make up the blockchain. A chain is formed by connecting each block. There are three parts to every block. Information on transactions, the parties involved, and the cryptographic algorithms thatdistinguish one block from another are all contained in ablock. There are four basic steps that explain how blockchain works. a) Transaction execution b) Transaction Verification and validation c) Transaction storage in blocks d) Block hashing and blockchain integration.

For blockchain technology to work, it requires a network of interconnected digital ledgers that record all financial transac- tions in real time. Every single transaction, from start to finish, is recorded in the blockchain ledger. Every transaction is validated using a distinct ID to create a block, and the owner's private key securely protects the user's data. The distinctive fingerprints of each brick link them together. According toXu et.al[91]), consensus is a procedure that helps with the validation and linking of block chains. Hence, the data stored in the block can store many types of real-time data, including as digital assets, contract details, and authorized financial transactions.

A. Blockchain Architecture

1) Application Layer : A blockchain's "highest layer" refers to its most topmost layer. Users are able to interact with the system through its graphical user interface. Ethereum,Solidity, Parity, and a few others are among the tools. Data recorded on a blockchain cannot be tampered with since it is both transparent and immutable. No one can get in or do anything dishonesty-related. There are two levels that make up the application layer: the application layer itself and the execution layer. To interact with the blockchain network, end users employ the application layer. Many parts, including application programming interfaces (APIs), user interfaces (UIs), frameworks, and others, make up the application layer. All of the smart contracts, rules, and chain code are located at the execution layer. The rules and the code that is now running are included in this sublayer. It is the application layer that communicates with the execution layer and relays the instructions. At this layer, we have security issues related to the centralized nodes that process cryptocurrency transactions. Problems with server security include distributed denial of service attacks, unauthorized access to the server, breaches in host security, and password cracking. That is why it is so important for app developers to check their code for known vulnerabilities and run thorough tests.[44]

2) Data model: The data model ensures that cryptocurrency structures are simple and direct. Every application has its own unique data model. Included in the data set are records of transactions as well as master and reference records. It includes the physical storage, data structure, and distributed database of the blockchain. Blockchain transactions are struc- tured into blocks in a decentralised network. Changes to data are not possible unless both parties consent. Two main parts make up the blockchain data structures: linked lists and pointers. A pointer is a reference to another variable's location. The linked lists formed by the chained blocks have connections between each block and the block before it. Hashing is the building block of a Merkel tree. Within each block, you'll find the Merkel root, which stores details like the version number, nonce, and information about the previous block. Thecomputing power of the people participating in the network is what makes the blockchain secure. As an incentive for

individuals to actively participate in the network nodes, the blockchain usually compensates them with digital currency. On the other hand, centralization becomes an issue when members refuse to work together on this.

3) Network layer: The P2P layer is another name for the network layer. In a peer-to-peer (P2P) network, individual computers work together to accomplish a common goal. The nodes carry out the transaction on the blockchain. Full nodes and half nodes are the two types of nodes. To ensure the min- ing rules' validation, transaction, and verification processes, a full node is used. By enabling communication, propagation, and discovery among all nodes, the P2P layer guarantees that the blockchain network status is correct and up-to-date. This entity's primary role is to facilitate the transmission of trans- actions between peers. Efficiently using the available network bandwidth for transmission is an important consideration.

4) Execution Layer: The program's execution will include the implementation of the contract. Many contracts should be efficiently and predictably executed within a single transactionblock. Deterministic execution of transactions is employed to forestall inconsistency. According to Sturm et al. (2019),[79] the Caterpillar engine is a blockchain execution engine that provides a number of features, such as the ability to deploy process models, create instances for those models, and control and record the execution of those instances. Contract negotiation, verification, and implementation can be facilitated by a smart contract that operates within the blockchain net- work. Smart card implementation provides improved security and reliability without taking third-party costs into account.[81] Concerns about this layer relate to security holes and threats that smart contracts might encounter. Assaulting the control flow of the contract and breaking the atomicity of the transaction are the goals of the assault. Inadequate permission checks or a lack of explicit function accessibility are the most common causes of these attacks, which allow an attacker to access or change a variable or function that shouldn't be accessible. Therefore, taking precautions against known vulnerabilities before developing smart contracts is essential to reduce the likelihood of data manipulation and increase trust. A battery of security checks have to be run on it before it can be released. Experts must immediately optimize code, audit.

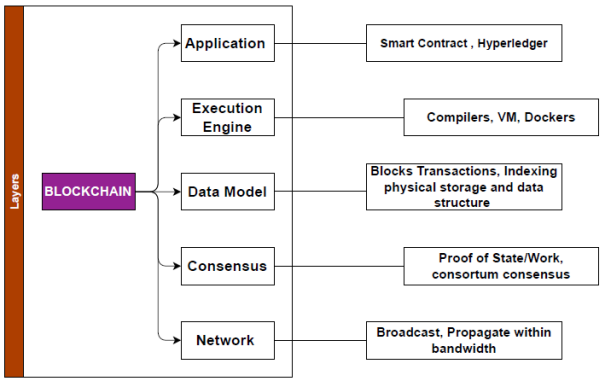

Fig. 3: Blockchain Layers.

code frequently, and actively watch for any unusual behavior displayed by deployed contracts if they want to reduce losses.

5) Consensus layer: When it comes to blockchain design, the consensus layer is king. "Conclusion algorithm" is the name given to the consensus algorithm. A blockchain can- not exist without a consensus algorithm. Using a consensus algorithm, the blocks are verified. There are many layers in a blockchain, but this one is considered the most important. To create a set of rules for transactions that all users agree upon is the main job of the consensus layer. For the purpose of information verification, globally recognized sets of trans- actions are specified. Blockchain consensus algorithms fall into one of two categories: permissionless or permissioned. Networks like as Ethereum and Bitcoin are examples of permissionless blockchains, which are also called probabilistic models. Permissioned is the second type; it follows a deter- ministic approach similar to Hyperledger Fabric. Nodes in a blockchain network check the authenticity and correctness of orders placed by other nodes. Various types of assaults, such as bribe attacks, long-range attacks, and Sybil attacks, might compromise the consensus layer. So, it's critical to look intoa faster and more reliable consensus mechanism while also making it more resistant to current threats.

V. APPLICATION OF BLOCKCHAIN IN HEALTHCARE Thanks to innovations like industry 4.0, the healthcare sector has grown substantially. Improved patient data management and easier healthcare research have prompted a shift away from paper-based systems and toward electronic healthcare records and electronic medical records. Modern innovations like as telemedicine and the IoMT are reshaping healthcareas we know it. The healthcare business might be drastically affected and even transformed by blockchain technology. Every link in the healthcare supply chain stands to benefit from blockchain technology. Raw material suppliers, logistics companies, manufacturers, wholesalers, and service providers all fall into this category. Electronic health records (EHR) sys-tems also exist for the purpose of evaluating and authenticating

patient data. Among the many potential uses for blockchain technology in healthcare is the enhancement of mobile health apps, the development of monitoring equipment, the storage and exchange of electronic medical records, the documentation of clinical trials, and the management of insurance policies.[40]

Researchers and healthcare practitioners face challenges with incomplete data, sluggish communication, and insuf- ficient workflow tools. Xiang et.al (2022)[90], note that another issue is the absence of reliable connections that might connect all standalone healthcare systems to create a com- pletely accessible end-to-end network. According to Zheng et al. (2018)[99], the healthcare industry is encountering difficulties in efficiently storing and safeguarding electronic health records. Decentralization and virtual anonymity made possible by blockchain technology will allow for trustless transactions to take place. Data integrity is guaranteed by this feature, which prevents a single entity from altering or du- plicating entries. Using blockchain technology, we can ensure the safe transfer of sensitive information including medical records, test results, treatment histories, episodes, diseases, and ambulance services. Quickly checking the digital signatures of all users and adding them to the ledger accomplishes this.[96] However, there are many challenges to implementing blockchain technology in the healthcare industry because toits intricacy.

According to Holbrook (2020)[37], Hyperledger Fabric, a distributed ledger across networks, is the solution for organiza- tions to share information in this EHR. Cryptocurrency com- panies including Ripple, Ethereum, Quorum, Corda, NEO, and NEM are among many that have released their own Blockchain platforms. The use of robotics and wireless communication networks to allow doctors to execute actual surgeries remotely is known as telesurgery.[86] Under the general category of telemedicine, this procedure is included. In addition to alleviating the doctor shortage, this strategy also helps save time and money. One blockchain-based application that aspires to enhance decentralization in several industries is Medblocks.[74]

A. Drug Supply and Traceability

A large number of people get hurt or die every year because they took fake medications. Medications that are not authentic can cost pharmaceutical businesses a lot of money and ruin their reputation. Instead of utilizing a traditional supply chain management system, blockchain-based medication traceability can improve supply chain efficiency by preventing fraud and the spread of counterfeit goods. A drug traceability system was created by Musamih et al. (2021)[61] that enables stakehold- ers to track medication through the use of a smart contract. The on-chain resources, decentralized storage system, and smart contract will all be accessible to stakeholders through software devices. An application programming interface (API) will connect the front end, which is a decentralized app (dApp), to the back end, which is a smart contract, on-chain services, and decentralized storage system. To ensure the security of public health data and to promote the sale of transparent medicines, Tseng et al. (2018)[82] developed a G-coin blockchain.

B. Tracking Medical IoT Device

A world where all devices are able to communicate and interact with each other through data is what the internet of things (IoT) envisions.[97] Many different types of intelligent devices and systems are finding widespread use in various sectors, including but not limited to smart homes, wearables, smart cities, smart grids, and autos. Large volumes of data are being generated by the expansion of the Internet of Things (IoT). An important challenge is keeping the data's reliability. By establishing a distributed service that is authorized by all participants, blockchain technology can be utilized to establishtrust in IoT data. This keeps the data safe and immutable.

Internet of Things (IoT) data can be made more secure and transparent through the use of blockchain technology in healthcare. It can also pave the way for future improvements in scalability, standardization, and efficiency in the IoT. To prevent hackers from gaining access to their data and to keep tabs on who has accessed it, patients will be able to set permissions on blockchain-enabled IoT devices used in healthcare. Depending on the precise conditions detected by Internet of Things (IoT) sensors, smart contract-backed blockchain systems can automate payments along the supply chain.

A lot of people are getting into the idea of using the Internet of Things (IoT) in healthcare to help both patients and doctors. This would include attaching sensors to little gadgets that would track patients' vitals and gather data for analysis. The widespread adoption of IoT has the ability to turn healthcare facilities into "smart hospitals," automating many processes for doctors and nurses. According to Kumar et al. (2023)[48], a blockchain-managed healthcare system that makes use of the Internet of Things (IoT) can guarantee the safe flowof data. The proposed method uses zero knowledge evidence to ensure secure data transfer and data integrity. The use of Ethereum smart contracts eliminates the data security issues related to the interplanetary file system. The major objective of this approach is to maintain privacy and secrecy of healthcare data transmitted through the blockchain. Furthermore, this technology addresses the authentication, consensus latency, throughput, delay, and security level issues plaguing healthcare blockchains. A variety of patient data forms, including text, speech, and images, can be safely stored, processed, and transmitted online through the use of smart particles and multimedia integration into healthcare infrastructure. Ahad et al. (2020)[3] suggested a multimedia data processing system for healthcare IoT to address the unique challenges of data management and

data protection. Simplifying the enrollment process for diagnosis and guaranteeing secure and efficient transactions are two examples of the healthcare industry con- cerns that this system aims to address. To address privacyand security concerns in fog-IoT, Baucas et al. (2023)[14] proposed a private blockchain with federated learning. The fundamental goal of the fog-IoT network is to address the issues of adaptability, privacy, integrity, and security that come with wearable Internet of Things sensors.

Tracking medical devices from their inception to their even- tual decommissioning is another vital strategy to revolutionize healthcare. It can be difficult for hospitals to keep track of all the different pieces of medical equipment that different departments and patients utilize. In a medical emergency, getting the right resources quickly is of the utmost importance. In order to avoid unnecessary repurchasing and fraudulent actions from the beginning of the supply chain all the way to decommissioning, it is essential to have efficient systems in place for tracking and monitoring medical devices.[42] When compared to more conventional methods of location monitoring, there are many advantages to using a blockchain- based approach. Blockchain stands out because to its inherent immutability and tamper-resistance. Regulatory compliance can be enhanced with the use of blockchain technology, which can create an immutable record of the device's location, history of movement, maker, reseller, and serial number. This blockchain-based approach successfully foils any malicious attempts to modify or remove a device's location history from the database. The use of blockchain technology enables us to gather crucial data regarding the utilization of loaned medical equipment, confirm their presence in authorized areas, and guarantee that clients utilize them. The capacity to automate the usage process, maintain an inventory history, and quickly find equipment in an emergency are all benefits.

C. Health Insurance Claims(HIC) processing

Health insurance is becoming a need for most individuals as a result of the rise in health concerns. The enormous costs associated with medical emergencies might make it difficult for individuals with minimal financial means to cope. A person can rest easy knowing they won't go into debt if they have health insurance because it safeguards their finances and helps pay for unexpected medical bills. Issues of privacy, fraud,and security could surface when discussing health insurance. The massive costs that fraud causes for people, organizations, and governments have made it a hotly debated topic in the health insurance industry recently. Therefore, it is critical for businesses and governments to invest in systems that can detect fraudulent events and transactions.

Insurance claim processing is notoriously difficult and time-consuming due to the many moving parts involved, such as checking the legitimacy of claims, collecting data from various sources, and dealing with consumer reports of abandoned policies. It takes a long time and involves a lot of steps altogether. Insurers can manage risks and gain control of insured assets using this technology in a secure and transparent way.[27] For the time being, transactions are crucial to the insurance system. In order to address the concerns about se- curity and efficiency, many Fintech systems use an immutable ledger to identify cases of cryptocurrency double-spending. Blockchain technology is used to create this ledger (Raikwar et al., 2018). Two insurance service models are available in the blockchain-based system: one that protects end-users' personal web identities and another that protects the data security of commercial websites. Web identity security is the primary emphasis of the second approach. A copy of the claim's supporting documentation is automatically uploaded during authentication. The policyholder and insurer automatically enter into contracts to improve their trust in each other.[34]

D. Vaccine Distribution, Tracking, and Registration

To stop the spread of contagious diseases, vaccination is the best option. Vaccine supply chains are distinct from more traditional ones due to the perishable nature of the products and the necessity for stringent shipping and storage regulations to ensure the safety of individuals.[26] Inadequacies, such inefficient delivery methods or a lack of compatibility, lead to the suspension or delay of vaccination supplies. When a pandemic breaks out, governments must quickly launch a mass vaccination campaign, which requires them to set up an appropriate logistical network and distribute a lot of vaccine doses efficiently.

Inadequate storage space, outdated medical facilities, and a lack of qualified medical staff are all examples of phys- ical constraints. To ensure the preservation of the vaccines, specialized storage equipment is necessary. Because of their limited capacity and availability, ultra-freezers must be man- aged efficiently if vaccines are not to expire. Unpredictability in vaccine supply and demand due to breakdowns in com- munication between supply chain participants can exacerbate regional imbalances and inefficiencies. Particularly in light of the possibility of cyberattacks or tampering, it is critical to guarantee the security of health data.

To evaluate how blockchain technology could improve supply chain performance, a simulation model was created. This strategy uses smart contracts to automate procurement processes and increase communication among parties. Previ- ous vaccine distribution criteria served as the basis for this.[70] The desire for the nationwide vaccination program led to its development. The constructed simulation model allowed for the smart contract-based automation of the vaccination procurement process. Using smart contracts, we were able to keep tabs on each region's inventory and set up

and execute appropriate inventory policies. Sookhak et al. (2021)[78] found that by implementing transparent and integrated data sharing throughout the supply chain, vaccine distribution be- came more efficient, leading to a decrease in inventory levels. In an effort to slow the spread of the virus, governments around the world instituted lockdown procedures. It was a huge task for healthcare experts to oversee the vaccination and testing process for the populace. It is critical to optimize operations to increase efficiency and save more lives. Smart contracts were created to automate the process of capturing and documenting events relevant to the distribution and delivery of COVID- 19 vaccinations, ensuring data traceability. A Digital Vaccine Passport (DVP) system was proposed as a means of handling the pandemic's severity. Andrew et al. (2023)[9] state that this system's goals include using blockchain technology to automate the issuing of testing certificates and prioritize the provision of safe vaccines to people who need them. With the use of the private blockchain Hyper-ledger Fabric, the DVP system made testing and vaccination a breeze, taking advantage of the distributed ledger technology's increased privacy, transparency, and credibility. The system improved efficiency while decreasing costs.

E. Data Management of Patient

There has been a lot of use of blockchain technology in healthcare data management, with the main goals of making it more secure and efficient. According to Pillares et al. (2019)[65], medical records, patient appointments, billing, and accounting are all aided by electronic storage. Lab testing are also conducted electronically. They are widely utilized in healthcare-related Electronic Health Record (EHR) sys- tems. Our top priority is to ensure the provision of safe, immutable, and cross-platform accessible medical records. Using blockchain technology, a full medical record can be kept for every patient, guaranteeing the safe capture and storage of all relevant health data. Patients, doctors, regulators, healthcare facilities, and insurance companies all play a part in making this happen.

F. Health waste and supply chain management

In the wake of the COVID-19 epidemic, healthcare waste management has emerged as a major challenge. The accumu- lation of waste from hospitals and vaccines is the main cause of the increase in garbage. One strategy to fight COVID-19 is to have everyone wear a face mask. In addition to wearing protective gear, health care personnel must put the safety of their patients and coworkers first. There has been an alarming increase in hospital trash, which is adding to environmen- tal contamination, because the majority of masks are made of non-renewable petroleum-based materials. Sharps, tainted blood, tissue and organ fragments, chemicals, medications, and radioactive materials are all part of healthcare waste. A popular strategy for healthcare waste management is reverse logistics (RL), which includes the collection, sorting, and disposal of non-hazardous and hazardous materials from product pack- aging and other items. When it comes to assessing medical facility trash and aiding in ecological management, Healthcare Waste Management indicators are invaluable. According to Veisi et.al (2022), the researchers prioritized the criterion and used the Analytic Hierarchy Process (AHP), a technique for multi-criteria analysis, to set weights for several variables.[84] The purpose of the established evaluation method was to identify the most important signs of waste.

Mass vaccination production results in an extra type of waste due to overproduction and underutilization of vac- cines. Present data management methods and technologies for COVID-19 vaccinations are deficient in key areas including trust, security, accountability, traceability, and transparency. As a result, a five-stage blockchain-based solution was proposed. The entire waste lifecycle, from consumption to production to disposal, is covered by the blockchain system. There are a number of smart contracts that monitor every step of a COVID-19 vaccine's life cycle to make sure everyone is held accountable for their actions and to cut down on wasteful overproduction, underordering, or underconsumption. Accord- ing to Musamih et al. (2021),[61] the REMIX IDE was used to create the Ethereum-based smart contract, which was then deployed to the Kovan Testnet. The proposed approach enhanced data processing performance by utilizing the PoA consensus algorithm and effectively handled the difficulty of storing and managing vast amounts of data. A private permis- sioned Ethereum blockchain was used to achieve enhanced data privacy. By utilizing a private permissioned blockchain devoid of centralized authority, regulators were able to adapt the blockchain's configuration to their needs and make use of smart contracts. The commitment smart contract ensures that all entities are responsible for their own garbage, leading to a decrease in overall waste.

Healthcare providers are tasked with effectively managing the Healthcare Supply Chain (HCSC) process, guaranteeing its efficacy in both routine daily operations and pandemic scenarios like COVID-19. On a daily basis, items are trans- ported both domestically and globally, yet healthcare prac- titioners continue to encounter difficulties with procedures like as procurement, ordering, forecasting, and distribution, despite substantial advancements in new treatment alterna- tives and technology. Similar to manufacturing supply chains, healthcare operations face significant challenges when trying to be optimized and managed. The healthcare supply chain (HCSC) isn't complete without group purchasing organiza- tions (GPOs), which help with vendor selection and provide volume discounts to providers. In order to streamline the management of GPO contracts and improve the efficiency of the contracting process in HCSC, Omar et al. (2021)[63] suggested a blockchain-based solution that uses Ethereum smart contracts and a decentralized storage

system. Through a blockchain-based GPO contract solution, the same decentral- ized Ethereum network may link healthcare providers, GPOs, distribution, and manufacturers. The solution streamlines the essential processes involved in obtaining pharmaceuticals and medical equipment. With the proposed architecture, trustwor- thiness and transparency were guaranteed, and only authorized parties could access smart contracts. By eliminating pricing discrepancies among stakeholders, the solution improved cost efficiency.

A well-functioning and open distribution network that all relevant parties can examine is crucial for the success of a global immunization campaign and the speedy introduction of a vaccine. Food, commodities, and pharmaceutical drugs are just a few of the vaccine supply chain goods that might get damaged while in transit. There are a number of potential causes for this, including incorrect storage methods, exposure to air or sunshine, and an inappropriate environment for storage. By making transportation networks more transparent and open, the Internet of Things (IoT) has made shipment monitoring more efficient. According to Alkhoori et al. (2021), one of the main ideas behind CryptoCargo is to use blockchain technology to monitor container conditions throughout trans- portation and identify any infractions that could compromise the cargo's safety. The use of smart contracts to record these violations on the blockchain makes it more reliable in a scenario with several parties and low levels of trust because the blockchain is a secure and immutable storage system.

Vaccine manufacturers provide the correct conditions for vaccine distribution, and smart contracts make sure that every node in the network is aware of these requirements. In order to make vaccine administration easier, Antal et al. (2021)[11] developed a prototype that includes a clear solution for side effects and is tamper-proof. The prototype underwent testing on the Ropsten Ethereum test network. Every on-chain action's results were confirmed and verified using the Ether- scan platform. The findings of an implementation based on Ethereum show that it is feasible in terms of gas consumption and the number of transactions executed. Better efficiency and openness in the distribution of COVID-19 vaccinations were the outcomes of the proposed method's successful resolution of the campaign monitoring issue. It further guaranteed the ability to track and do an exhaustive audit of the circumstances of storage and delivery. The registration and administration of the vaccination waiting list were guaranteed to be open and accurate. The most recent firms that have used blockchaintechnology for healthcare services are compared in Table 4. The following table details the most recent market leaders that provide blockchain-based healthcare system solutions.

VI. CONSENSUS ALGORITHMS IN HEALTHCARE

A. Proof-of-work (PoW)

According to Vukolic´ (2015)[87], the idea of Proof-of-Work(PoW) was first put forward by D. Work in 1993. To accept a block, the most frequent strategy is the one that many peers take. Due to the lack of a central authority in a decentralized network of peers to validate or verify transactions, the selec- tion of a participant to authenticate a transaction is vital in the establishment of a blockchain.[2] Before a block can be added to the chain, it must first be verified by each individual peer. A miner is an independent peer or node with the capacity to confirm and aggregate all transactions into blocks. The process of carrying it out is known as mining. This tactic entails giving the miners a difficult puzzle to solve, which will take a lot of time and energy yet is easy to verify. We use a number of randomization techniques based on trial and error to solve the problem before we generate the proof of work. The miner who fixed the problem can now create a new block and verify the transactions. One way to handle the input values is to use hashing. Including the hash of the previous block in the current block becomes a computationally expensive procedure when the network traffic is high and there are many users. Because it is necessary to recreate the blocks that came before it in order to generate a new block, the likelihood of doing so is limited. So, it's impossible to tamper with the data. Both Bitcoin and Ethereum use the Proof-of-Work consensus mechanism. The healthcare IoT services are not usable because of the high bandwidth requirements, even though they are widely used.

B. Proof-of-stake (PoS)

An alternate paradigm to the Proof-of-Work (PoW) consen- sus mechanism, the Proof-of-Stake (PoS) idea first emerged in 2012. The idea of Proof-of-Stake (PoS) was established to solve the problem of the high processing requirements of solving the cryptographic challenge in Proof-of-Work (PoW).[43] In order to minimize the use of computer resources, the protocol was developed; it is called a probabilistic protocol. In this model, all nodes in a decentralized network with a large enough coin holding can join the mining pool and help ensure the legitimacy of transactions. The more coins a miner has, the more powerful they are. As an example, a miner can only mine 20% of the blocks in the chain if they own 20% of the total coins in the blockchain. It is the responsibility of the miner with the most coins to verify and authenticate the transactions. If consumers only have a tiny amount of coins, the single miner technique won't work since it's too centralized and the miner controls the blockchain 100% of the time. Increasing the number of miners is one way to improve security and lessen the likelihood of fake stake attacks. A healthcare system would benefit greatly from PoS due to its minimal hardware requirements and energy consumption.

C. Practical Byzantine Fault Tolerance (PBFT)

The consensus technique known as Practical Byzantine Fault Tolerance (PBFT) was developed in 2002 by Castro and Liskov.[18] Its primary function is to deal with blockchain networks that contain nodes that are either partially trusted or otherwise problematic. PBFT's efficiency and complexity have made it famous. With the use of request and answer messages, nodes in this system run in an asynchronous fashion. Even when certain nodes in a dispersed network aren't working well and may have erroneous or correct information, the network can nonetheless reach an agreement. When using PBFT to transmit a message, there are five separate steps to take. The relevant messages are the following: request, pre- prepare, prepare, commit, and response.[52] The client sends a message to the main node requesting something. Each node in the network receives a request message from the central node and relays the response to the client. This model isn't scalable and works well with a smaller network of nodes. A message overhead is the exponential growth in the number of messages sent and received as a network grows. Most of the time, enterprise networks make use of technologies like Hyperledger Fabric and Tendermint. M. C. Castro and Liskov (2010) and others have developed a method to mimic the algorithm that can survive byzantine errors. To reduce the impact of software bugs and dangerous attacks, the Byzantine fault tolerance technique is essential. Hyperledger Fabric with Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm that Dhillon et al. presented in 2017[25] that can handle as much as one-third of malicious Byzantine nodes. Prepared, committed, and pre-prepared are the three main stages that make up the procedures. In order for a node to move on to the next stage, it must represent at least two- thirds of all nodes. For this reason, the network must be able to identify each node. Hyperledger and similar third- party regulated private blockchains are ideal candidates for this method. However, open, decentralized blockchains that do not require permission are not the best fit for them because of their slow growth and inability to handle bad activities. Data processing speed, transmission latency, and the amount of computer resources needed to run the PBFT consensus algorithm are all significantly improved. Its features make it an excellent choice for use in healthcare systems.

D. (dBFT)Delegated Byzantine Fault Tolerance

It is flexible and works similarly to PBFT, except it doesn't need all nodes to participate to add a new block. As soon as the number of abnormal nodes drops below a specific level, PBFT ensures that the system is live and secure. A more trustworthy and accurate consensus is achieved by PBFT when contrasted with other protocols. Nevertheless, PBFT's complexity makes it inefficient, especially when dealing with a large number of nodes. Some nodes are designated to act as representatives for other nodes in the dBFT protocol (ontology/consensus/dbft at master · ontio/ontology· GitHub, 2023) that is currently in use. These officials follow a procedure for reaching a consensus that is similar to PBFT. Consequently, blockchain systems in healthcare can benefit from this concept. When you delegate jobs or responsibilities to other people at random, you are engaging in delegated randomization. To integrate blockchain into large-scale asynchronous network applications, Zhan et al. (2021)[94] propose Byzantine fault tolerance (DRBFT). The nodes that will run the PBFT protocol are selected at random using a rigorously unbiased approach. All three of these criteria—unpredictability, uniform distribution, and impartiality—are satisfied by the proposed approach.

E. Proof-of-capacity (PoC)

PoC is an improvement to PoW, which stands for Proof-of- Work. Allocating dedicated computing resources and enough storage space is essential for Proof of Concept (PoC) mining, which is necessary for the mining of following blocks. Because of its unique features, Proof of Concept (PoC) is more effective than Proof of Work (PoW). Providers of services are allotted memory space by PoC. As a miner, you can use this idea to trade your free disk space for money on a decentralized network. With more room to work with, more people are likely to take use of the service offered in exchange for their mining output. Since it uses just the current memory space to validate blocks, the Proof of Concept (PoC) model uses less energy than other models. Although it may come as a disappointment, the method is being promoted as a more environmentally friendly substitute for older algorithms used for consensus mechanisms, including proof of work (PoW). This mining strategy is currently being implemented by Burst- coin. Among the many advantages of PoC are its low energy consumption, low maintenance needs, low cost, decentralized network structure, shorter mining times, and space reusability. Its lesser level of security, limited research possibilities, and preference for people who gather large amounts of space are some of the limitations that come with it. On the other hand, healthcare system node selection is flawed since it prioritizes capacity above all else.

F. (LPoS) Leased Proof-of-Stake An improved variant of Proof-of-Stake (PoS), Leased Proof-of-Stake (LPoS) debuted in 2018.[75] LPoS fixes PoS's centrality problem. A leasing option makes it possible for nodes that don't have enough money to participate in block verification. In a leasing arrange- ment, those with more wealth can lend it to others with less wealth for a set period of time. Nodes with low balances have a better chance of solving a block, and wealth holders will keep as little ownership as possible throughout the leasing term. All of the people that have money will get a proportionate share of the prize when these nodes solve a block. The system's decentralization and security are both improved by this. The financial incentives that LPoS relies on make it less applicable to healthcare IoT. Other e-healthcare services, though, work wonderfully with it.

G. Proof-of-elapsed-time (PoET)

A network of users can decide on mining privileges and take on the job of validator using this alternate consensus mechanism. In this setting, the chances of any given participant becoming a validator are equal. This feature is activated via a timer, and each participant is given a unique duration. Every- one gets a random waiting time, and the first person whose timer runs out, even if it's small, gets to add a new block to the blockchain.[64] This approach uses a simple methodology that doesn't require a lot of computing power. But, in order to set the time using this method, specific hardware is required. Businesses that use distributed hyperledger systems on a wide scale use this concept.

H. Proof-of-importance (PoI)

To choose the most trustworthy node to validate trans- actions, Proof-of-Importance (PoI) adds reliability to Proof- of-Stake (PoS). Unlike the Proof of Stake (PoS) consensus process, there is no guarantee that the person with a larger stake can influence the chain's blocks. The approach considers a node's reputation—determined by a set procedure—and the quantity of transactions involving that node, among other criteria, rather than depending only on node balances to identify the next winning node. There is minimal delay and consistently good payouts from the Point of Interest (PoI). In addition, it makes very little demand on computer and network resources. Because of these features, PoI is a good fit for healthcare systems. Customers can also utilize the ratings and reviews of medical facilities to help them choose.

I. Activity Proof (PoA)

Combining elements of Proof of Work (PoW) and Proof of Stake (PoS), Proof of Activity (PoA) serves as a consensus mechanism. In the Proof of Work (PoW) consensus algorithm, known as a cryptographic hash function, miners compete to be the first to solve it and secure the next block in the blockchain. In contrast, the solved block will be devoid of any transactions and will merely include the miner's address and a header. The addition of transactions to the block is followed by the selection of validators who will use the solved block's header to sign the new block, so achieving consensus. Proof of stake allows this to happen. Improved defenses against attacks are a benefit of this method, but the additional latency it can cause might be a dealbreaker for healthcare apps that rely on instant decisions.

J. Proof-of-Burn(PoB)

One method is the Proof of Burn (PoB) technique, which entails sending funds to an unrecoverable address. The number of bitcoin that miners have burned determines their priority in solving the following block. Although this method works well for creating cryptocurrency, it isn't suitable for use in healthcare networks because it requires a financial system and coin burning, neither of which are present. A cryptocurrency called Slimcoin uses PoB.

K. Paxos consensus algorithm

To get a unanimous decision across several decentralized systems, one can employ the Paxos consensus algorithm. The challenge of reaching an agreement in decentralized net- works was the inspiration for the Paxos consensus algorithm. In the face of ambiguity, paxos stands as a metaphor for reaching a compromise. Even if a network partitions or a server goes down, the Paxos algorithm will keep distributed systems running as expected. De Prisco et al. (2000)[24] states that distributed storage can operate consistently and reliably, like a thread-safe data structure, if a client application can connect to important roles in the distributed system. To accomplish a number of Paxos' attributes, the idea of a ballot is fundamental. With every purchase, a ballot acts as a distinct identifier. Separate tracking of Paxos ballots is maintained for each partition key. While overall throughput and availability do improve in the absence of coordinated transactions, a mutual order is not guaranteed. It is not possible for transactions to traverse partitions. The coordinator, who is also the node in charge of carrying out the transaction, starts by making a new ballot and requesting storage from the nodes that handle the data for that particular range of tokens. Replicas won't keep a ballot that's more recent than the one known, and the coordinator won't move on if the original doesn't respond to the copy. The coordinator is responsible for keeping all information up-to-date and allowing the change of a single transaction at a time. Paxos is a popular choice when there's a requirement to copy and maintain huge datasets, such databases or files, for an extended period of time. Even with a small number of unresponsive duplicates, the approach aims to develop. It takes a lot of processing power to run the Paxos algorithm. It was for this reason that the Raft consensus algorithm was developed.

L. multi-paxos consensus algorithm

For distributed systems, the multi-Paxos algorithm is an extension of the Paxos algorithm. Paxos promises to pick one of the suggested values. When it comes to picking a sequence of values or attaining consistent ordering of a set of values, the multi-paxos consensus technique proves to be invaluable in a distributed system. Through the use of the Multi-Paxos protocol, the leader is chosen to launch the proposal. An efficient two-step procedure can be reduced to one if the leader starts all the ideas; this eliminates the need to prepare. There is no need for a designated leader in Multi-Paxos. Instead, it ensures security while allowing multiple leaders to make requests at the same time. Improving the Multi-Paxos protocol by skipping the preparation phase and jumping straight to the acceptance one will allow uninterrupted proposal. By enabling the processing of numerous transactions, multi-paxos improves the blockchain's efficiency.

M. Raft consensus algorithm

Raft is an improved version of the Paxos algorithm that achieves consensus. According to Singh et al.

(2022)[76], it is designed to handle larger networks and uses a leader- based strategy to reach consensus. In the Raft consensus algorithm's closed distributed environment, the main server is called the leader and the other nodes are called the followers. Data updates and replication of transition logs are the leader's responsibility. Assuming it is functional and adjustable, the leader responds to client requests by periodically sending heartbeat signals to all followers. Some followers will notify their coworkers and push for an election if the leader becomes unreachable for whatever reason (death, network failure, etc.). Selecting a leader, duplicating logs, and guaranteeing safety are all basic components of consensus that Raft streamlines to make them more understandable. Furthermore, it guarantees a higher degree of consistency to lessen the amount of states thatneed to be taken into account. New entries are added to the log by the leader, who subsequently transmits the data to the otherservers. Since the leader is the only weak point in the system, setting up node fail over is essential for availability. The Raft consensus algorithm's method for choosing a new leader is called leader election. Assumption: All nodes participating in this process are trustworthy and not out to harm anyone.

N. Zab consensus algorithm The ZooKeeper Atomic Broadcast consensus method is known as Zab. According to Flavio etal. (2011)[41], it was custom-built to help the ZooKeeper coordination service recover from crashes. The three stages of Zab are discovery, broadcast, and synchronization. Processes carry out this protocol iteratively. The process can choose to end the current iteration and begin a new one at any timeby going to the discovery phase. According to the protocol,the Zab process might take on either the main or secondary roles. A leader not only completes the primary's broadcast call sequence-based duty, but also proposes transactions in the same order. The protocol specifies a series of steps that follow- ers must follow in order to validate and process transactions. Also, a leader carries out the orders of their followers. To determine who could take the helm, each procedure makes useof a leader oracle. When a process is in the discovery phase, it asks its leader oracle for advice on what to do next. With the help of Zab, the primary process executes client actions while the backup processes receive the incremental adjustments that are required. This is how ZooKeeper implements a primary- backup system. Because the sequence in which updates are generated impacts an incremental state change, Zab must ensure that in order to deliver a specific state change, it must first give any other changes on which it depends.

O. Proof of Learning (PoLe)

The development of autonomous neural network (NN) ar- chitecture, along with the growth of the network and training data, has led to significant performance increases in deep learning. According to Liu et al. (2021)[54], the Proof of Learning (PoLe) method re-allocates the computing power used for block consensus to improve the optimization of neural networks. The consensus nodes use the training andtest data to build neural network models, demonstrating their learning capabilities. The entire blockchain network is then given access to these datasets. A linear neural network layer called a secure mapping layer (SML) was added to PoLe to prevent consensus nodes from cheating. The blockchain is updated with a new block whenever the network reaches a consensus. Improved transaction processing and reliable block generation were two outcomes of the PoLe protocol's study.

P. Proof-of-deep learning (PoDL)

Chenli et al. (2019)[21] created proof-of-deep-learning (PoDL), a consensus approach, to make multi-access edge computing (MEC) applications more secure and private. Any application that uses a Proof of Work (PoW) consensus technique can implement Proof of Distributed Ledger (PoDL). To keep blockchains running, the algorithm stops wasting time on pointless hash calculations and starts using deep learning techniques. By gradually adding components to block headers, the PoDL can be used to any PoW that is based on cryptocurrencies. Energy recycling blockchain is implemented via PoDL in the proposed approach. The training dataset is used to train the deep learning models, while the test datasetis used to evaluate their accuracy.

Q. Seperate Proof-of-deep learning (s-PoDL)

Separate proof-of-deep-learning (S-PoDL) was introduced as a computationally efficient consensus method by the authorsLuo et al., 2021.[57] To speed up the creation and deploymentof blocks in blockchain-enabled MEC applications, the S- PoDL used a two-stage computation approach that made use of an accounting technique. The S-PoDL technique divides each node into several parts so that several deep-learning models can be trained. Getting N nodes to agree on who is responsible for keeping the books is the consensus method. The accounting authority grew in inverse proportion to the number of modes. By shortening the time it takes to generate blocks, the S- PoDL improved throughput. There was an improvement tothe consensus conclusion and a reduction in the extra burden.

R. Dynamic random byzantine FaultTolerance (DR-BFT)

One of the most difficult problems with edge computing is data integrity. In a dynamic network, where nodes canjoin or exit the blockchain network at any time, most current consensus methods can't handle edge computing. Data security in edge computing was enhanced with the introduction of the Dynamic Random Byzantine Fault Tolerance (DR-BFT) consensus mechanism.[29] Through the use of data transfers to servers located at the edge of a network, edge computing increases processing speed and decreases the load on data centers. Data Correctness Validation, String

Consensus, and Binary Consensus are the three sub-algorithms that make up DR-BFT. Guaranteed agreement, validity, and termination were accomplished with minimal system overhead when the DR-BFT algorithm was applied to a dynamic network.

VII. PRIVACY AND SECURITY CHALLENGES

There is an inherent security to blockchain technology. The data stored in blockchain cannot be changed or altered, making it extremely secure. Also, the platform uses cryptographic proofs to make sure the blockchain can't be hacked and a very effective consensus technique to make decisions. Blockchain technology has a great degree of security and is immutable, yet it still has its flaws.

A. Replay Attack

The intentional or fraudulent delay or repetition of legitimate network messages is called a replay attack.[36] Cyberattacks come in many forms; one of them is the replay assault, which goes by several names including replaying or replicating attack. When an adversarial actor intercepts valid data in transit over a network, the data is effectively duplicated. An attack for cross-chain transactions that takes use of the fact that two forked cryptocurrencies are compatible with one other and allows transactions to be verified on both chains. Security systems mistook the assaults for normal data exchanges since the supplied data was authentic. The term "time stamping" describes a method of continuously adding timestamps to data. To avoid repeat attacks, this technique is employed. There is a potential for the private key to be revealed when the blockchain produces it during the signature process. In their 2018 study, Huang et al.[38] proposed a solution dubbed LNSC to tackle this problem. To guarantee that the key is changed every time, this approach generates temporary private keys for each session. The hash function is made more difficult to decipher by using elliptical curve encryption.

B. Sybil Attack

An individual launches a Sybil assault when they create many accounts on a network with the goal of taking over the network and endangering its security. This kind of attack, which goes by the name "account creation abuse," happens when someone tries to make a lot of social network accounts. A network node in a P2P network can run multiple identities at once. The main goal of this assault is to get control of the network and use it for malicious purposes. Multiple identities can be created and managed by a single computer. Proof of Each new block added to the network is checked for legitimacy using Bitcoin's work consensus method. The eclipse attack aims to target a single node as its primary purpose. One possible countermeasure to this kind of assault is the "Trust Chain," which Wen et.al(2021)[89]) suggest using Proof of Work (PoW) is a method used by the Trust chain to confirm that the transaction is legitimate. The trust chain creates a temporary immutable chain to fix this problem. Such Sybil attacks are detected and countered using the consensus algorithm. To determine who is trustworthy and reliable in an online community, a consensus algorithm and a trust chain work together.

C. False data injection attack

In a fake data injection attack, the sensor triggers an erroneous event that did not actually occur because it detected an attack. Due to the erroneous data being generated, the system's data is being steered in an uncontrollable direction. Distributed voting algorithms, proposed by Liao et al. (2023)[50], use consensus mechanisms to improve communication between nodes and so reduce the impact of this danger. The veracity of a node can be verified by any other node. Accurate data is produced when all nodes reach a unanimous agreement. When all the nodes agree that there is negative agreement, it means that there was false data injection.

D. Tampering attack

The application data can be modified by exchanging certain parameters between the client and server. The application data contains many kinds of information, such as product details, user credentials, and permissions. There are several copies of the data, if any is present at all. Since there are many duplicates and no single authoritative copy is necessary, this dispersed data provides protection against manipulation attempts. There is a chance that the Bitcoin address can be manipulated if any attacks take place. Wang et al. (2020)[88] used a public-key cryptosystem to thwart these kinds of attacks. They presented a method called a homomorphic Paillier encryption strategy to hide data, including transactions, and maintain the confidentiality of amounts. The non-spendable account that is created using this encryption method can receive bitcoin transactions but cannot spend them. A positive sum for both the inputs and the outputs indicates that the transaction is equal. An attack could happen if the scenario has negative- sum outcomes. The following method can be used to detect a tampering assault.

E. Impersonation Attack

The goal of an impersonation attack, which is also called a collusion attack[72], is to obtain sensitive information from a person or business using email in order to share it with a corporation. Impersonation attacks, such as corporate email compromises or CEO attacks, are quite widespread. CEO fraud is an example of an assault that zeroes in on a specific company or person. The use of a seemingly legitimate- looking email in an impersonation attack is a common tactic. Exposure of the private key allows an authenticated user to conduct unlawful operations. If you want to steal money, you can start an impersonation attack. Validation of transactions, preservation of user privacy, and concealment of user personal information are all guaranteed by this technique. For the purpose of detecting and identifying these particular types of attacks, Ling et al. (2018)[51] presented an ECDSA technique. Only authorized users are able to

generate valid signatures using ECDSA, an attribute-based signing technique. The impersonation attempt will be exposed if the related operation fails.

F. Man in the middle attack

A central intermediary, such a person or a server, can facilitate communication between multiple individuals. There is always one hub for these kinds of communication. Any intermediate communication channel is used to convey in- formation from user A to user B. The party acting as an intermediate between A and B may alter and send data to the other side. It is possible for two sources to transmit erroneous information to each other. The term "Man-in-the- Middle attack" describes this specific type of attack. A security mechanism between two entities called mutual authentication was introduced by Lin et al. (2018)[51] to combat this attack. Ellipsoidal curve encryption is employed by Huang et al. (2018)[38] to provide security.

G. DDoS Attack

Distributed denial of service is shortened to DDoS. You might think of this as a DoS assault in its most basic form. In a Distributed Denial-of-Service (DDoS) assault, several computers work together to overload a single web server's resources. The goal of this kind of assault is to overwhelm the targeted system by simultaneously flooding it with more traffic than it can handle.[85] Attacks affecting traffic, bandwidth, and applications are all part of distributed denial of service attacks. A distributed denial of service attack's principal objec- tive is to prevent authorized users from reaching the website. Attackers need to overwhelm the victim server with requests for a distributed denial of service assault to be successful. A distributed denial of service (DDoS) assault use several systems to overwhelm the targeted systems, in contrast to a denial of service (DoS) attack that employs a single machine and a single internet connection.

H. Double spending attack

If an attacker wants to get more money, they can use the same Bitcoin to execute several transactions. This is called a double spending assault. A multi-signature transaction, first proposed by Aitzhan et al.(2018)[5], is a method for spending tokens that involves the use of multiple keys. The timestamp is used by Wang et al. (2020)[88] to detect the attack and the Proof of Work (PoW) technique is used to defeat it. Thus, by implementing these methods, double-spending attacks can be successfully reduced. For a transaction to be legitimate, the user needs to validate it quickly. All cases of double-spending assaults should be mitigated by implementing this technique. It loses all utility after the user confirms the transaction.

I. Refusal to sign Attack

Any agency, good or evil, can decide to support or reject a deal. When he realizes a transaction won't benefit him, he'll opt out. It is possible to take precautions against this type of attack, even though no concrete measures have been proposed to reduce or eliminate it. To sidestep unsavory characters or break the deal into manageable chunks,Wen et al.,(2021)[89] presented a method.

VIII. IMPROVEMENTS IN PRIVACY AND SECURITY

It is critical that all nodes on the blockchain have access to all data for data verifiability and traceability. Nevertheless, this method brings up issues related to privacy. By associating real addresses with anonymous network addresses, attackers can gain access to the transaction data stored on individual nodes, so jeopardizing privacy. One frequent tactic for easing privacy worries is anonymization. The anonymization method keeps the transaction's core functionality intact while remov- ing any identifying information. In addition, data saved on the blockchain cannot be changed or erased once it is made available to the public; this makes it accessible to everyone without the need for security measures. The very nature of the blockchain network makes it vulnerable to security threats. Because of this, strengthening the blockchain network's secu- rity and privacy is of the utmost importance. Hash functions, homomorphic encryption, public key cryptography, a trusted execution environment, zero-knowledge proof, and safe multi-party computation are all technologies that enhance security and privacy. Because they are recorded on the blockchain, smart contracts automatically take on the network's privacy features. Smart contracts on the blockchain rely on a variety of cryptographic methods for privacy protection.

A. Zether

Bünz et al.(2020)[16], introduced Zether in 2020; it is a decentralized model for hidden payments. While Ethereum and Libra are similar, Zether stands out due to its trustless mechanism within smart contracts that allows users to make payments while protecting their anonymity. Zether uses cryp- tographic proofs to guarantee the anonymity of transactions. Zether relies on zero knowledge proof, which enhances inter- operability via a ZK-proof technique called -Bullets. Zether allows for the smooth interaction of any number of smart contracts, which simplifies processes like voting, payment channels, and consensus. Zether has a lot of issues, the most obvious of which is its high price. Another issue with Ethereum's gas mechanism is the potential breach of privacyit introduces.

B. Proof-of-work framework

The safety of blockchains is a byproduct of their per- formance improvement. The PoW consensus algorithm's performance-security tradeoff was investigated by Ferrang et al. (2016).[31] To examine the security and efficiency tradeoffs associated with Proof of Work (PoW) parameters, a new mathematical approach is proposed. The idea that no one should have control over more than half of the computing capability is central to

Proof of Work (PoW) security. Reason being, such kind of person might theoretically take over the system if they always kept the longest chain. The main parts of the suggested quantitative framework are a security model and a PoW blockchain simulator. Consensus and network settings are inputs to the PoW blockchain. Stale block rate, block propagation time, and throughput are the metrics used to measure the blockchain's efficiency. Input to the security model from a Proof of Work (PoW) blockchain includes security settings as well as the stale block rate. It ensures the best possible adversarial strategy and safety protocols. Chain forks, caused by outdated blocks, compromise the blockchain's security and performance. The development of the main chain is impeded by them, and its performance and security are greatly endangered. On the one hand, the network's adversary gains an advantage due to stale barriers. On the flip side, blocks that aren't actively mining tend to waste more data transmission and rarely receive any rewards for their work. The proposed architecture improves the blockchain's defenses against attacks like eclipse attacks, double spending, and selfish mining.

C. SmartPool

Luu et al.(2017) first suggested the SmartPool solution for mining pools[59] The problem that SmartPool is trying to address is that pool administrators now have too much control over the powerful computing resources that their users have access to. At present, just ten mining pools command at least ninety-five percent of Bitcoin's mining power, while six pools command eighty percent of Ethereum's. Attacks on cryptocurrencies like as 51% attacks, network partitioning, and double spending originate from these vulnerabilities. At the moment, the get block template protocol is the only way that bitcoin pools let miners choose which transactions to include in their blocks. Miners can opt to mine an empty block or a set of transactions chosen by the pool; this protocol does not provide any additional functionality beyond this. This is especially problematic on Ethereum, because miners participating in managed pools do not have the legal right to reject the operator's chosen selection of transactions. To solve this problem, instead than depending on centralized miners, a decentralized network of miners might be used in place of the pool protocol. However, they cannot be used on the Ethereum blockchain. This is why SmartPool exists: to use a decentralized pool of efficient and scalable miners to increase the safety of the Ethereum coin. To make sure the verification procedure is secure and efficient, an expanded Merkle tree is used. Miners are given the freedom by SmartPool to choose which transaction they would like to see included in the block. Decentralization, equity, efficiency, and security are the four pillars upon which the SmartPool protocol rests.

D. Enigma

With anonymity as its primary goal, Enigma is a decentralized computing platform. A secure multiparty computation approach allows verified secret exchange, which is the foun- dation of the system. A decentralized computation platform called Enigma enforces the anonymity of its computational model using a highly optimized variant of Secure Multi-Party Computation (SMPC). A verifiable secret-sharing system is put into place to do this. Enigma encrypts private data stored off-chain and securely transmits confidential information via a personalized distributed hash table. Similar to Bitcoin, Enigma enables autonomous data management and protection without relying on reliable third parties. When compared to more con- ventional blockchain redundancy methods, Enigma's method of data distribution is unique. Every node in the Enigma network keeps an exact copy of all transactions. Enigma and the blockchain both run the code. Unlike blockchain technology, which can only guarantee accuracy, Enigma's execution guarantees both secrecy and completeness.

E. Oyente

Smart contracts can process hundreds of dollars' worth of virtual currency efficiently, creating strong financial incentives that entice competitors. On the other hand, smart contract plat- forms like Ethereum run on open networks, so anybody may join without needing permission, unlike traditional distributed application platforms. This makes traditional permissioned networks, including centralized cloud services, vulnerable to attacks that aim to control system operations. A symbolic execution tool called Oyente was proposed by Luu et al. (2016)[58] to find security flaws in smart contracts built on Ethereum. The Oyente tool accepts the smart contract's bytecode and the Ethereum global state as inputs. At first, the CFG Builder will analyze the bytecode and statically create the smart contract's Control Flow Graph (CFG). In order to simulate the execution of a smart contract using Ethereum state and CFG data, EXPLORER employs static symbolic execution. By identifying non-constant jump targets during symbolic execution, the technique seeks to enhance and enrich the Control Flow Graph (CFG). Issues with reentrancy vulnerability, timestamp dependence, mishandled exceptions, and transaction ordering dependence are all within Oyente's capabilities to handle.

F. Ekiden

The complexity and lack of confidentiality of smart con- tracts causes them to function poorly. To address the issues with smart contracts, zero knowledge proof systems and secure multi-party computing were employed. Nevertheless, the procedure is complicated due to the complex structure of the cryptography algorithms. By securely isolating apps within the environment and implementing a Trusted Execution Environment (TEE), a workable solution to the issue outlined earlier can be achieved. Ekiden, a blockchain system that prioritizes privacy and confidentiality, was created by Cheng et al. (2019)[20] to address the difficulty of utilizing TEE for blockchain applications.

Trusted Execution Environments (TEEs) are the foundation of Ekiden's computations, which guarantee secrecy and make possible the effective application of robust encryption methods like functional encryption and black box obfuscation. Reliable sources can also be randomly assigned using TEE. To run smart contracts on processing nodes that deal with private data off the main blockchain, Ekiden uses Trusted Execution Environments (TEEs). After that, it checks the smart contract execution with a remote attestation protocol to make sure it was accurate. In order to keep information private, make sure everything is reliable, and make smart contracts perform better, Ekiden shows that blockchains and trusted enclaves are two parts of a larger security puzzle that, when coupled, can form a strong and flexible framework.

G. Hawk

To address the privacy issues that have arisen as a result of smart contracts, the Hawk framework was created.[7] To avoid explicitly storing transactional information on the blockchain, Kosba et al. (2016)[45] presented a decentralized smart contract framework. Developers can partition the contract into its private and public parts using the Hawk framework. Financial and personal information that should not be made public is kept in the private part of the data, while other information that can be made public is kept in the public part. There are three main parts to the Hawk program. They are the core blockchain software that every node, user, and administrator runs. The Hawk manager is a dependable go- between that keeps user data private, both outside and inside the smart contracts. In the case of an accident, the hawk management has the power to stop the protocol, and users can receive appropriate compensation.

H. Town Crier

Smart contracts often necessitate communication with non- blockchain data sources. The reliability of the data presented by these sources is, however, not guaranteed. Smart contracts do not have a digital signature or network connectivity, even if HTTPS seems to be a solution to this issue. Town Crier is a mechanism proposed by Zhang et al. (2016)[95] for the purpose of verifying the data streams of intelligent contracts. Town Crier (TC) is structured with a TC contract and a TC server. The TC contract mediates communication between the client and the TC database. Electronic signature and verification of data streams acquired from web sources is TC's principal objective. Ensuring gas sustainability and establishing a trustworthy computing foundation are two of TC's key security objectives. Data sources, the TC contract, an enclave, a relay, a blockchain, and network connectivity make up TC's security architecture. When it comes to com- municating between the enclave, blockchain, and network, the relay module is your best bet. The TC system is designed tobe stable and functional even when the relay is intentionally attacked. Hence, TC ensures that data streams are protected and kept confidential.

IX. DISCUSSIONS, CHALLENGES RESEARCH OPPORTUNITIES

The healthcare industry has great potential to benefit from the implementation of blockchain technology, thanks to its prominent qualities of decentralization, immutability, con- sensus processes, and enhanced capacity. This article intro- duces the notion of blockchain technology and its potential use in healthcare systems. The qualities of blockchain arevery compatible with the needs of the healthcare business, making the integration of blockchain technology in health- care inevitable. Initially, the characteristics of blockchain are introduced in relation to healthcare systems. Furthermore, we elucidated the diverse applications of blockchain and its relevance, with a particular focus on the healthcare sector. The uses of blockchain technology in healthcare include patient data management, drug traceability, cryptocurrency payment, clinical trials and data protection, and secure healthcare se- tups. The many categories of blockchain, including permis- sioned blockchain, permissionless blockchain, and consortium blockchain, are elucidated in relation to healthcare blockchain systems.

The consensus process is a fundamental characteristic of blockchain technology. The several consensus algorithms are introduced, along with their suitability for use in the healthcarefield. Table 8 presents a comparative examination of different consensus algorithms and their respective properties. We have observed that several consensus algorithms are not appropriate for the healthcare sector due to their restrictions, including large bandwidth requirements, significant power consumption, and transmission delays. Ultimately, we discussed the security obstacles that arise in the context of blockchain technology. While blockchain is indeed safe and unchangeable, there remain some unresolved security challenges. To enhance the potential of blockchain for healthcare applications, it is crucial to thoroughly assess the security challenges during the deploy- ment process. Table 10 presents a comprehensive comparative examination of the security attacks. Additionally, we will explore the difficulties and potential areas of study in the fieldof healthcare blockchain technology.

This section outlines the difficulties and potential areas for further investigation that arise from the analysis of existing research in this article. Here are some of the most common difficulties that demand extensive research and attention.

A. Data privacy

The primary characteristic of blockchain is its transparency. Given that the user's transaction is easily trackable and visible,it is necessary to provide safeguards to ensure the privacy of the transaction for users.[15] Each user should be allocated a unique private key for every transaction to prevent attackers from deducing any

real coins or information from the cryp- tocurrency. A methodology utilizing blockchain technology is suggested to safeguard social network data while maintaining anonymity. This architecture employs a distributed blockchain system to safeguard sensitive information, while non-sensitive information is handled by the core system. The paper by Zhang et al. (2020)[98] presents a novel approach for addressing the issue of data synchronization. Data security and efficiency are guaranteed by utilizing a stochastic homomorphic elliptic curve cryptography encryption paradigm. Nevertheless, ensur-ing data privacy poses a significant obstacle in the context of blockchain, particularly when it involves healthcare data. Healthcare data comprises confidential personal information that requires safeguarding. The disclosure of any type of personal information would have an impact on the individual. Therefore, it is necessary to prioritize research on blockchain technology in order to ensure the privacy of health data. The study of ensuring tamper-resistance and non-repudiation in e-health systems is a recently emerged field in the health- care business. A Privacy Preserving Biometric Authentication (PPBA) system was developed to safeguard patient privacy during healthcare service access by implementing anonymous patient authentication.[71] This blockchain-based solution provides secure biometric identification with processing and offline encryption using an encrypted domain architecture. A public blockchain is utilized to host the necessary infrastruc- ture for online authentication, ensuring the integrity of the data. The approach reduces the transaction count necessary for authentication, permits the revocation of biometric identities, and incorporates auditing capabilities for malicious individu-als. The results indicated that the proposed architecture effec- tively protected against these attacks, even when the templates were stored in an encrypted form. The PPBA system, which is built on blockchain technology, utilizes transaction fees as a means to discourage hill-climbing attacks. The General Data Protection Regulation (GDPR) requires that the utilization of biometric data be maintained as confidential. The GDPR ensured the secure private matching of sensitive biometric data by employing the identical cryptographic technique. The utilization of secure drawings, which are verifiably secure procedures for protecting biometric templates, was employed for this purpose. The integration of blockchain-based PPBA systems has enabled the prevention of attacks by ensuring data integrity and facilitating audits.

B. Scalability and Size of blocks

The block size is the maximum capacity for filling a block with transactions. If the network surpasses its capacity, the block will be rejected. A blockchain is a form of distributed database that operates without a central authority. Conse- quently, a distributed ledger refers to a system where every node processes every transaction and stores a complete copy of the ledger's current state. Within the healthcare system, it is sufficient to have only the pertinent ledgers for specific nodes, rather than a full replica of the ledger.[49] The block size issue is exemplified by unprocessed patient data, including genomes and key organs. Although larger data packets on the blockchain incur higher storage expenses, they provide a greater amount of data that can be audited on the blockchain.[19] Therefore, it is crucial to preserve equilibrium in the ongoing storage and exchange processes. Another significant obstacle in the implementation of blockchain technology is ef- fectively managing the decentralized system with a substantial number of peers. The magnitude of the transaction is immense. Consequently, both the transaction processing rate and the latency of communication see an increase. The time between transaction submission and confirmation is influenced by the consensus protocol.

C. Node count and system responsiveness

A node in a blockchain-based system is a constituent ele-ment. It serves as the foundation of technology and represents anything connected to the network. As the number of nodes in the network increases, the internode latency increases in a logarithmic manner with each additional node. Moreover, in the field of Communication, as the quantity of nodes increases, the quantity of computational resources also increases. In the healthcare industry, it is anticipated that large communities would be interconnected, utilizing blockchain technology. Due to the increasing adoption of blockchain technology, there will be a significant proliferation of transactions that will be generated and documented. Once all parties involved reach a consensus on each transaction pertaining to the ledger, the blockchain-distributed ledger will incorporate new transac- tions. Despite its seeming complexity, this strategy is effec- tive due to the limited size of the blockchain.[6] Certain entities who engage in temporary data exchange apply pre- authorization fees as a means to decrease the memory require- ments on the blockchain. As the user base of the blockchain network expands, the system's responsiveness diminishes. Due to the high number of players, achieving consensus from all participants is necessary for even a single transaction.

D. Data analysis and visualization

Examining and deriving insights from the blockchain net- work is intricate. An essential aspect for private enterprises is the analysis and collection of data on digital money, which is necessary to meet the requirements of intelligence analysis and management.[23] It aids in the detection of suspect activities during fraud, security, and compliance investigations. The seven challenges in analyzing blockchain data are entity identification, privacy protection, network picture, networkvisualization, market effect analysis, illegal behavior detection, and transaction pattern recognition.[23]

E. Transaction and blockchain auditing

A blockchain transaction is a process of conducting busi-

ness with several participants in a network. Developers are constantly discovering the latest methods for performing blockchain transactions, which is driving the expansion of the blockchain sector. As the blockchain system scales to accommodate high transaction volumes, it encounters chal- lenges. Every transaction on the Ethereum blockchain requires validation from every validator in the network. This is a factor that contributes to the network's subpar performance due to the amount of data being processed. Consequently, the process of obtaining a consensus or verifying digital identification will be time-consuming. Examining a blockchain involves dealing with several intricacies. Real-time analysis is challenging because to the potential occurrence of forks, which undermines the dependability of the data. Efficient financial reporting and audit procedures are necessary for network management. If a consensus is reached by the majority of participants, it is still possible for the written records to be tampered with and for the blockchain to be reconstructed. From this standpoint, it becomes exceedingly challenging for a regulatory body to conduct an audit of blockchain and verify whether the data and transactions have been tampered with or not. Securing the data and preventing vulnerabilities from unauthorized users is a difficult task.

F. Consensus algorithm selectivity

The consensus algorithm is a system that facilitates unan- imous agreement among all participants in a blockchain net- work over a specific message. It also guarantees the accuracy of the most recent block added to the chain. The system must ensure that the message saved by the peer does not give rise to any fork attack and that it stays safeguarded from malicious attacks. A transaction is deemed legitimate if the consensus among peers confirms its legitimacy. Nevertheless, reaching a successful agreement with a substantial number of users is challenging and requires a significant amount of effort. As an illustration, every validator on the Ethereum blockchain is required to verify each transaction. The network speed may be slower depending on the amount of data being processed. In addition, because to its irreversible characteristics, blockchain may not be ideal for some applications. During certain circum-stances, the blockchain system faced difficulties in addressing certain patient issues, such as the lack of predictability in accessing the system. In addition, a surgeon was previously not allowed to access their data during an emergency. Due to the lack of adequate ways, patients frequently hesitate to participate or grant authorization for data exchange. In such scenarios, it is necessary to have a fair time in order to obtain a prompt response from the system, as well as consensus from all involved parties about crucial transactions.

G. Cost of transmitting data

Blockchain-based data transmission solutions facilitate the transfer of both small and large files by circumventing chal- lenges related to nonrepudiation in safe data transportation.[32] While data transmission is a common feature in most Internet-based applications, only a small number of them prioritize confidentiality as a component of data security. When a data transmission scheme is conducted without the authorization of a third party or a central computer, conflicts can easily arise during the transmission of important data, particularly digital products, because a dishonest participant can deny the occurrence of a specific data transmission event. Signing and encrypting can be employed to address the afore- mentioned challenge. In contrast, digital signature systems often rely on public key infrastructure (PKI), which introduces additional intricacies in managing certificates and renders them impractical for distributed networks.[4] The blockchain technology has offered a potent instrument for accomplishing automated data transfer. Although blockchains do not have a central authority for data storage, they nonetheless necessitate some form of authority. Due to the inherent characteristics of the health-care sector and the sensitive nature of its data, the implementation of blockchain applications will heavily depend on the enforcement of regulations, monitoring, and adher- ence to established standards and procedures. The consensus process of any blockchain is not contingent on technology, but rather on a consensus reached among the participants. Blockchain is being employed to create novel and advanced solutions for improving the existing standards of medical data and personal health record management, sharing, and processing. Blockchain technology is undergoing a conceptual transformation in the healthcare industry, where it has proven to be valuable in terms of improved efficiency, remote access, technical innovation, personal privacy, and data management security.[8]

H. Commercial uses

The utilization of blockchain technology in commercial applications is highly sought after and offers a multitude of advantages. Bitcoin is widely recognized as the pioneering application of blockchain technology in the business sec- tor. Non-financial blockchain applications encompass a wide range of sectors such as securities clearance, logistics, HR management, healthcare, strategic planning, personal database administration, and more. Regarding Business as a Service (BaaS), the blockchain technology is utilized in diverse in- dustries. There would be numerous instances in which BaaS may be utilized. The suitability of an application for BaaS (Blockchain-as-a-Service) is determined by the combined ad- vantages it gains from both blockchain technology and services.[77] The several fields in which blockchain technology can beutilized. The manufacturing sector is the initial industry that seeks to produce things that can be easily traced. Utilizing BaaS for food tracking is a suitable application to ensure the traceability of food and the verification of checkpoints prior to reaching the final customers. In this scenario, BaaS could help by providing data about the food source and ensuring the food remains uncontaminated during its

transportation from the sender to the recipient. The second area pertains to e- payments that adhere to pre-established regulations or con- tracts. As an illustration, the act of compensating publishers with royalties. Understanding the timing and method of royaltypayments is crucial. Due to the utilization of smart contracts, the blockchain is well-suited for a BaaS (Blockchain-as-a-Service) application. This is because predetermined conditions may be integrated into the smart contract to facilitate the automation of these payments. The financial management of a corporation is categorized as the third domain. Examples of BaaS solutions include those that offer financial management and product traceability. It offers comprehensive traceability and anti-counterfeiting solutions that help organizations tackle issues including data manipulation and lack of transparency. The fourth domain refers to a public ledger or information- sharing system that is unchangeable, can be verified, and requires authentication.

I. Legislation and rules

While the blockchain has brought about significant changes in society, it has also presented legal institutions with novel obstacles. Owing to the newness of blockchain technology and the delay in legal oversight, it gave rise to a multitude of legal challenges, especially during its initial phases of advancement.[55] A comprehensive understanding of theattributes of the blockchain facilitates the development and enhancement of legislation and regulations pertaining to the blockchain. Several governments are adopting blockchain technology and strengthening regulatory measures. Examples of challenges include delegation of authority, legal interpretation and ju- risdiction issues, privacy protection and online real identities issues, reliability and deletion rights issues, and transparency and personal data privacy difficulties. Moreover, technology and law serve as interchangeable alternatives in the realms of national and social government.[56] the expense of a technological solution is lower than that of a legal solution in a social context, the technical instrument can replace the legal form as the principal means of generating orders. Blockchain technology, which uses distributed databases and smart contracts, has the potential to overcome technical and legal obstacles and establish innovative governance systems.

X. FUTURE DIRECTIONS

Considering the future of blockchain technology and its potential as a career path for individuals with expertise in the field is crucial. Blockchain is an immutable and tamper- proof digital ledger that securely records transactions in a verifiable manner. Many companies from various sectors havebeen attracted to the potential of blockchain technology and its applications. The incorporation of blockchain technology into various fields of study has the potential to gain international acceptance, thanks to its disruptive characteristics.

Due to its inherent characteristics, blockchain technology is expected to gain significant traction in the field of cybersecu- rity in the future. Although the Blockchain ledger is openly accessible and decentralized, the data remains secure and capable of being verified. Cryptography is employed to encrypt data in order to prevent illegal tampering and enhance security. Centralized systems are susceptible to significant risks such as data loss, hacking, and human error. Blockchain technology has the potential to enhance the security and resilience of cloud storage systems against hacking attempts.

The efficacy of blockchain technology in tracking financial assets has been established. Multiple financial institutions made investments in this technology upon recognizing its potential and observing its favorable outcomes. The transpar- ent ledger architecture of blockchain allows it to effectively manage the movement and transactions of illicit funds. Given these achievements, governments worldwide are already ex-ploring the possibility of utilizing blockchain technology to enhance their control over national finances and economy. Moreover, the utilization of blockchain technology can be highly beneficial for governmental entities as it facilitates the efficient handling of large quantities of data.

Enterprises are employing blockchain technology to con-struct a decentralized network of Internet of Things (IoT) devices. By incorporating blockchain-based solutions into IoT access control, it becomes possible to oversee device-to- device communication and manage various processes suchas software upgrades, error handling, and monitoring energy usage.

Utilizing blockchain technology enables the monitoring of hiring, spending, and releases at each phase of the supply chain, hence decreasing delays and minimizing human er-ror. By implementing traceability, blockchain technology can guarantee the legality and fair trade certification of products. The utilization of blockchain technology has the capacity to mitigate financial losses resulting from the trade of illegalitems.

Currently, international trade is discouraged due to its inefficiency and lack of organization, which hampers the flow of business. Foreign trade is also abundant with flaws, deceit, and counterfeiting. By implementing blockchain technology, we can effectively address many of these problems by includ- ing cryptocurrencies. The consolidation of payment systems, paperwork, and regulation into a unified digital international system can effectively tackle a significant portion of fraud and inefficiency. This will inaugurate a novel epoch characterized by heightened commerce and enhanced global interactions.

Blockchain technology is progressing and expanding in various areas, such as cryptocurrencies and commercial

appli- cations including smart contracts, automated tracking, and rule enforcement. Blockchain will have significant implications for both corporations and society.

XI. CONCLUSION

Blockchain technology has the capacity to resolve certain challenges faced by the healthcare sector. The primary ad- vantage of blockchain technology in the healthcare industry lies in its well studied applications, which include security, integrity, decentralization, availability, and authentication prin- ciples. This is made possible by the global ledger and block- related architecture. The healthcare industry is facing chal- lenges in adapting to an increasingly advanced digital infras- tructure, which encompasses Internet-enabled devices, Internet of Things (IoT), smart devices, and sensor gadgets. Due to the capacity of these technologies to enhance the healthcare sector's ability to cater to patients in a more interconnected world, malevolent individuals can exploit weaknesses in these technologies to obtain and replicate data, thereby impeding the sharing of records among hospitals. This can result in outdated information, which can subsequently result in health complications or incorrect diagnosis, as well as challenges in verifying a patient's identity. The study evaluated data that suggests blockchain technology has the capacity to tackle nu- merous current obstacles in the healthcare industry. The goal isto empower patients by granting them control and possession of their medical data, enabling them to securely share it with anyone of their choosing. This article offers a comprehensive examination of the different aspects of blockchain, including its features, use cases, architecture, types, consensus methods for healthcare blockchain, security problems, and performance evaluation metrics. In addition, we conducted multiple com- parative assessments on the characteristics of blockchain and its utilization in healthcare applications.

The healthcare business may leverage the numerous ben- efits of blockchain technology to effectively tackle various challenges associated with data sharing and security. However, blockchain is not a universally applicable solution. Instead, a comprehensive examination of specific blockchain issues and their consequences for the healthcare sector is necessary. The healthcare business has not extensively examined the mining incentives, which play a crucial role in blockchain, as well as specific blockchain attacks that have the potential to halt the entire system. The promise of blockchain technology inthe health industry is over exaggerated and its worth may be overestimated. Blockchain does not solve the most challengingobstacles to the digital transformation of the health sector, such as the absence of data interoperability, and it does not offer any further advantages.

Although the data stored in blockchain-based ledgers is inherently secure and resistant to tampering, it does not ensure the accuracy or quality of the supplied data. In addition to user mistake, malevolent actors may attempt to influence individuals' decisions over providing consent and authorizing access to their data. This threat is particularly serious due to the growing prevalence of individuals who are physically and intellectually frail in older populations. The only means of controlling this vulnerability are governance, regulation, and enforcement.

Healthcare organizations are prohibited from retaining or transmitting sensitive information as a result of implementing Blockchain technology, which requires trust in data storage systems without the need for a neutral intermediary to verify a transaction. The integration of blockchain and AI technologies has the potential to elevate the quality of healthcare services. The reduction in medical sector expenditures will lead to increased accessibility and affordability of healthcare. The scarcity of experts is significantly hindering the widespread adoption of blockchain technology. Firstly, there is a shortage of personnel dedicated to innovation to adequately addressthe demand. Furthermore, the cost of recruiting existing blockchain experts is high. It is highly desirable for individuals to acquire a deeper understanding of Blockchain technology given its increasing prominence.

REFERENCES

1. Asad Abbas, Roobaea Alroobaea, Moez Krichen, Saeed Rubaiee, S Vi- mal, and Fahad M Almansour. Blockchain-assisted secured data man- agement framework for health information analysis based on internet of medical things. Personal and ubiquitous computing, 2024; 28(1): 59–72.
2. Shubhani Aggarwal, Rajat Chaudhary, Gagangeet Singh Aujla, Neeraj Kumar, Kim-Kwang Raymond Choo, and Albert Y Zomaya. Blockchain for smart communities: Applications, challenges and opportunities. Journal of Network and Computer Applications, 2019; 144: 13–48.
3. Mohd Abdul Ahad, Gautami Tripathi, Sherin Zafar, and Faraz Doja. Iot data management—security aspects of information linkage in iot systems. Principles of internet of things (IoT) ecosystem: Insight paradigm, 2020; pages 439–464.
4. Md Rayhan Ahmed, AKM Muzahidul Islam, Swakkhar Shatabda, and Salekul Islam. Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. IEEE Access, 2022; 10: 113436–113481.
5. Nurzhan Zhumabekuly Aitzhan and Davor Svetinovic. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing, 2016; 15(5): 840–852.
6. Jameela Al-Jaroodi and Nader Mohamed. Blockchain in industries: A survey. IEEE access,

7:36500–36515, 2019.
7. Maher Alharby, Amjad Aldweesh, and Aad Van Moorsel. Blockchain- based smart contracts: A systematic mapping study of academic research (2018). In 2018 International Conference on Cloud Computing, Big Data and Blockchain (ICCBB), pages 1–6. IEEE, 2018.
8. Davide Aloini, Elisabetta Benevento, Alessandro Stefanini, and Pierluigi Zerbino. Transforming healthcare ecosystems through blockchain: Opportunities and capabilities for business process innovation. Tech- novation, 2023; 119: 102557.
9. J Andrew, Deva Priya Isravel, K Martin Sagayam, Bharat Bhushan, Yuichi Sei, and Jennifer Eunice. Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications, 2023; page 103633.
10. J Andrew Onesimu and J Karthikeyan. An efficient privacy-preserving deep learning scheme for medical image analysis. Journal of Information Technology Management, 12(Special Issue: The Importance of Human Computer Interaction: Challenges, Methods and Applications.), 2020; 50–67.
11. Claudia Antal, Tudor Cioara, Marcel Antal, and Ionut Anghel. Blockchain platform for covid-19 vaccine supply management. IEEE Open Journal of the Computer Society, 2021; 2: 164–178.
12. Ankit Attkan and Virender Ranga. Cyber-physical security for iot networks: a comprehensive review on traditional, blockchain and ar- tificial intelligence based key-security. Complex & Intelligent Systems, 2022; 8(4): 3559–3591.
13. Meryeme Ayache, Amjad Gawanmeh, and Jamal N Al-Karaki. Dass-care 2.0: Blockchain-based healthcare framework for collaborative diagnosis in ciomt ecosystem. In 2022 5th Conference on Cloud and Internet of Things (CIoT), 2022; pages 40–47. IEEE.
14. Marc Jayson Baucas, Petros Spachos, and Konstantinos N Plataniotis. Federated learning and blockchain-enabled fog-iot platform for wear- ables in predictive healthcare. IEEE Transactions on Computational Social Systems, 2023.
15. Jorge Bernal Bernabe, Jose Luis Canovas, Jose L Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta. Privacy-preserving solu- tions for blockchain: Review and challenges. IEEE Access, 2019; 7: 164908– 164940.
16. Benedikt Bu¨nz, Shashank Agrawal, Mahdi Zamani, and Dan Boneh. Zether: Towards privacy in a smart contract world. In International Conference on Financial Cryptography and Data Security, pages 423– 443. Springer, 2020.
17. Daniel Burkhardt, Maximilian Werling, and Heiner Lasi. Distributed ledger. In 2018 IEEE international conference on engineering, technol- ogy and innovation (ICE/ITMC), pages 1–9. IEEE, 2018.
18. Miguel Castro and Barbara Liskov. Practical byzantine fault tolerance and proactive recovery. ACM Transactions on Computer Systems (TOCS), 2002; 20(4): 398–461.
19. Jiayuan Chen, Changyan Yi, Samuel D Okegbile, Jun Cai, and Xuemin Sherman Shen. Networking architecture and key supporting technologies for human digital twin in personalized healthcare: A comprehensive survey. IEEE Communications Surveys & Tutorials, 2023.
20. Raymond Cheng, Fan Zhang, Jernej Kos, Warren He, Nicholas Hynes, Noah Johnson, Ari Juels, Andrew Miller, and Dawn Song. Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In 2019 IEEE European Symposium on Security and Privacy (EuroS&P), 2019; pages 185–200. IEEE.
21. Changhao Chenli, Boyang Li, Yiyu Shi, and Taeho Jung. Energy- recycling blockchain with proof-of-deep-learning. In 2019 IEEE Inter- national Conference on Blockchain and Cryptocurrency (ICBC), pages 19–23. IEEE, 2019.
22. Kellie-Anne Crameri, Lynne Maher, Pieter Van Dam, and Sarah Prior. Personal electronic healthcare records: What influences consumers to engage with their clinical data online? a literature review. Health Information Management Journal, 2022; 51(1): 3–12.
23. Sabyasachi Dash, Sushil Kumar Shakyawar, Mohit Sharma, and Sandeep Kaushik. Big data in healthcare: management, analysis and future Marco Iansiti, Karim R Lakhani, et al. The truth about blockchain. Harvard business review, 2017; 95(1): 118–127.
24. Rateb Jabbar, Noora Fetais, Moez Krichen, and Kamel Barkaoui. Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity. In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 2020; pages 310–317. IEEE.
25. Flavio P Junqueira, Benjamin C Reed, and Marco Serafini. Zab: High- performance broadcast for primary-backup systems. In 2011 IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN), 2011; pages 245–256. IEEE.
26. Kadhim Takleef Kadhim, Ali M Alsahlany, Salim Muhsin Wadi, and Hussein T Kadhum. An overview of patient's health status monitoring system based on internet of things (iot). Wireless Personal Communi- cations, 2020; 114(3): 2235–2262.
27. Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19(1), 2012. prospects. Journal of big data, 2019; 6(1): 1–25.
28. Pingfan Kong, Li Li, Jun Gao, Kui Liu, Tegawende´ F Bissyande´, Roberto De Prisco, Butler Lampson, and Nancy Lynch. Revisiting the paxos algorithm. Theoretical Computer Science, 2000; 243(1-2): 35–91.
29. Vikram Dhillon, David Metcalf, Max Hooper,

Vikram Dhillon, David Metcalf, and Max Hooper. The hyperledger project. Blockchain enabled applications: Understand the Blockchain ecosystem and how to make it work for you, 2017; pages 139–149.
30. Lotty Evertje Duijzer, Willem Van Jaarsveld, and Rommert Dekker. Literature review: The vaccine supply chain. European Journal of Operational Research, 2018; 268(1): 174–192.
31. Christian Eckert and Katrin Osterrieder. How digitalization affects insurance companies: overview and use cases of digital technologies. Zeitschrift fu¨r die gesamte Versicherungswissenschaft, 2020; 109(5): 333–360.
32. Ismail Erol, Ahmet Oztel, Cory Searcy, and ˙I Tolga Medeni. Selecting the most suitable blockchain platform: A case study on the healthcare industry using a novel rough mcdm framework. Technological Forecast- ing and Social Change, 2023; 186: 122132.
33. Yuqi Fan, Huanyu Wu, and Hye-Young Paik. Dr-bft: A consensus algorithm for blockchain-based multi-layer data integrity framework in dynamic edge computing system. Future Generation Computer Systems, 2021; 124: 33–48.
34. Kurt Fanning and David P Centers. Blockchain and its coming impact on financial services. Journal of Corporate Accounting & Finance, 2016; 27(5): 53–57.
35. Mohamed Amine Ferrag and Lei Shu. The performance evaluation of blockchain-based security and privacy systems for the internet of things: A tutorial. IEEE Internet of Things Journal, 2021; 8(24): 17236–17260.
36. Thippa Reddy Gadekallu, Quoc-Viet Pham, Dinh C Nguyen, Praveen Kumar Reddy Maddikunta, Natarajan Deepa, B Prabadevi, Pubudu N Pathirana, Jun Zhao, and Won-Joo Hwang. Blockchain for edge of things: Applications, opportunities, and challenges. IEEE Internet of Things Journal, 2021; 9(2): 964–988.
37. Ahmad N Gohar, Sayed Abdelgaber Abdelmawgoud, and Marwa Salah Farhan. A patient-centric healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and iot. IEEE access, 2022; 10: 92137–92157.
38. Yurong Guo, Zongcheng Qi, Xiangbin Xian, Hongwen Wu, Zhenguo Yang, Jialong Zhang, and Liu Wenyin. Wischain: An online insurance system based on blockchain and denglu1 for web identity security. In 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), 2018; pages 242–243. IEEE.
39. Abid Haleem, Mohd Javaid, Ravi Pratap Singh, and Rajiv Suman. Medical 4.0 technologies for healthcare: Features, capabilities, and applications. Internet of Things and Cyber-Physical Systems, 2022; 2: 12–30.
40. Mustafa Maad Hamdi, Yuser Anas Yussen, and Ahmed Shamil Mustafa. Integrity and authentications for service security in vehicular ad hoc networks (vanets): A review. In 2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2021; pages 1–7. IEEE.
41. Joseph Holbrook. Architecting enterprise blockchain solutions. John Wiley & Sons, 2020.
42. Xiaohong Huang, Cheng Xu, Pengfei Wang, and Hongzhe Liu. Lnsc: A security model for electric vehicle and charging pile management based on blockchain ecosystem. IEEE access, 2018; 6: 13565–13574.
43. and Jacques Klein. Automated testing of android apps: A systematic literature review. IEEE Transactions on Reliability, 2018; 68(1): 45–66.
44. Ahmed Kosba, Andrew Miller, Elaine Shi, Zikai Wen, and Charalampos Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP), 2016; pages 839–858. IEEE.
45. Sreelakshmi Krishnamoorthy, Amit Dua, and Shashank Gupta. Role of emerging technologies in future iot-driven healthcare 4.0 technologies: A survey, current challenges and future directions. Journal of Ambient Intelligence and Humanized Computing, 2023; 14(1): 361–407.
46. K Suresh Kumar, T Ananth Kumar, AS Radhamani, and S Sundaresan. Blockchain technology: an insight into architecture, use cases, and its application with industrial iot and big data. In Blockchain Technology, pages 23–42. CRC Press, 2020.
47. Prabhat Kumar, Randhir Kumar, Govind P Gupta, Rakesh Tripathi, Alireza Jolfaei, and AKM Najmul Islam. A blockchain-orchestrated deep learning approach for secure data transmission in iot-enabled healthcare system. Journal of Parallel and Distributed Computing, 2023; 172: 69–83.
48. Gary Leeming, James Cunningham, and John Ainsworth. A ledger of me: personalizing healthcare using blockchain technology. Frontiers in medicine, 2019; 6: 171.
49. Zhuofan Liao and Siwei Cheng. Rvc: A reputation and voting based blockchain consensus mechanism for edge computing-enabled iot sys- tems. Journal of Network and Computer Applications, 2023; 209: 103510.
50. Chao Lin, Debiao He, Xinyi Huang, Kim-Kwang Raymond Choo, and Athanasios V Vasilakos. Bsein: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. Journal of network and computer applications, 2018; 116: 42–52.
51. MC Liskov. B (2010) practical byzantine fault tolerance miguel. Juvenile delinquency in Europe and beyond: results of the second international self-report delinquency study, pages 359–368.
52. Xiaoguang Liu, Ziqing Wang, Chunhua Jin, Fagen

Li, and Gaoping Li. A blockchain-based medical data sharing and protection scheme. IEEE Access, 2019; 7: 118943–118953.
53. Yuan Liu, Yixiao Lan, Boyang Li, Chunyan Miao, and Zhihong Tian. Proof of learning (pole): Empowering neural network training with consensus building on blockchains. Computer Networks, 2021; 201: 108594.
54. Kelvin FK Low and Eliza Mik. Pause the blockchain legal revolution. International & Comparative Law Quarterly, 2020; 69(1): 135–175.
55. Yang Lu. The blockchain: State-of-the-art and research challenges. Journal of Industrial Information Integration, 2019; 15: 80–90.
56. Xiong Luo, Pan Yang, Weiping Wang, Yang Gao, and Manman Yuan. S-podl: A two-stage computational-efficient consensus mechanism for blockchain-enabled multi-access edge computing. Physical Communi- cation, 2021; 46: 101338.
57. Loi Luu, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, and Aquinas Hobor. Making smart contracts smarter. In Proceedings of the 2016 ACM SIGSAC conference on computer and communications security, 2016; pages 254–269.
58. Loi Luu, Yaron Velner, Jason Teutsch, and Prateek Saxena. Smart Pool: Practical decentralized pooled mining. In 26th USENIX security symposium (USENIX security 17), 2017; pages 1409–1426.
59. Cristhian Martinez-Rendon, Jose Luis Gonza´lez-Compea´n, Dante D Sa´nchez-Gallegos, and Jesus Carretero. Cd/cv: Blockchain-based schemes for continuous verifiability and traceability of iot data for edge– fog–cloud. Information Processing & Management, 2023; 60(1): 103-155.
60. Ahmad Musamih, Khaled Salah, Raja Jayaraman, Junaid Arshad, Mazin Debe, Yousof Al-Hammadi, and Samer Ellahham. A blockchain-based approach for drug traceability in healthcare supply chain. IEEE access, 2021; 9: 9728–9743.
61. Xueli Nie, Aiqing Zhang, Jindou Chen, Youyang Qu, Shui Yu, et al. Blockchain-empowered secure and privacy-preserving health data shar- ing in edge-based iomt. Security and Communication Networks, 2022; 2022.
62. Ilhaam A Omar, Raja Jayaraman, Mazin S Debe, Khaled Salah, Ibrar Yaqoob, and Mohammed Omar. Automating procurement contracts in the healthcare supply chain using blockchain smart contracts. IEEE access, 2021; 9: 37397–37409.
63. Morgen E Peck. Blockchains: How they work and why they'll change the world. IEEE spectrum, 2017; 54(10): 26–35.
64. Iris Cathrina Abacan Pilares, Sami Azam, Serkan Akbulut, Mirjam Jonkman, and Bharanidharan Shanmugam. Addressing the challenges of electronic health records using blockchain and ipfs. Sensors, 2022; 22(11): 4032.
65. Eugenia Politou, Fran Casino, Efthimios Alepis, and Constantinos Patsakis. Blockchain mutability: Challenges and proposed solutions. IEEE Transactions on Emerging Topics in Computing, 2019; 9(4):1972–1986.
66. Igor Radanovic´ and Robert Likic´. Opportunities for use of blockchain technology in medicine. Applied health economics and health policy, 2018; 16: 583–590.
67. Nirmalee Raddatz, Joshua Coyne, Philip Menard, and Robert E Crossler. Becoming a blockchain user: understanding consumers' benefits re- alisation to use blockchain-based applications. European Journal of Information Systems, 2023; 32(2): 287–314.
68. Santosh B Rane and Yahya Abdul Majid Narvel. Data-driven decision making with blockchain-iot integrated architecture: a project resource management agility perspective of industry 4.0. International Journal of System Assurance Engineering and Management, 2022; 13(2): 1005–1023.
69. Marta Rinaldi, Maria Antonietta Turino, Marcello Fera, and Roberto Macchiaroli. Improving the distribution of covid-19 vaccines using the blockchain technology: the italian case study. Procedia Computer Science, 2023; 217: 366–375.
70. Neyire Deniz Sarier. Privacy preserving biometric authentication on the blockchain for smart healthcare. Pervasive and Mobile Computing, 2022; 86: 101683.
71. Jayasree Sengupta, Sushmita Ruj, and Sipra Das Bit. A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. Journal of network and computer applications, 2020; 149: 102481.
72. Shahid Munir Shah and Rizwan Ahmed Khan. Secondary use of electronic health record: Opportunities and challenges. IEEE access, 2020; 8: 136947–136965.
73. Salman Shamshad, Khalid Mahmood, Saru Kumari, Chien-Ming Chen, et al. A secure blockchain-based e-health records storage and sharing scheme. Journal of Information Security and Applications, 2020; 55: 102590.
74. Yenatfanta Shifferaw and Surafel Lemma. Limitations of proof of stake algorithm in blockchain: A review. Zede Journal, 2021; 39(1): 81–95.
75. Arshdeep Singh, Gulshan Kumar, Rahul Saha, Mauro Conti, Mamoun Alazab, and Reji Thomas. A survey and taxonomy of consensus protocols for blockchains. Journal of Systems Architecture, 2022; 127: 102503.
76. Jie Song, Pengyi Zhang, Mohammed Alkubati, Yubin Bao, and Ge Yu. Research advances on blockchain-as-a-service: Architectures, applica- tions and challenges. Digital Communications and Networks, 2022; 8(4): 466– 475.
77. Mehdi Sookhak, Mohammad Reza Jabbarpour, Nader Sohrabi Safa, and F Richard Yu. Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. Journal of Network and Computer Applications,

2021; 178: 102950.
78. Christian Sturm, Jonas Scalanczi, Stefan Scho¨nig, and Stefan Jablon- ski. A blockchain-based and resource-aware process execution engine. Future Generation Computer Systems, 2019; 100: 19–34.
79. Justin Sunny, Naveen Undralla, and V Madhusudanan Pillai. Supply chain transparency through blockchain-based traceability: An overview with demonstration. Computers & Industrial Engineering, 2020; 150: 106895.
80. Muhammad Tahir, Muhammad Sardaraz, Shakoor Muhammad, and Muhammad Saud Khan. A lightweight authentication and authorization framework for blockchain-enabled iot network in health-informatics. Sustainability, 2020; 12(17): 6960.
81. Jen-Hung Tseng, Yen-Chih Liao, Bin Chong, and Shih-wei Liao. Gov- ernance on the drug supply chain via gcoin blockchain. International journal of environmental research and public health, 2018; 15(6): 1055.
82. Sarah Underwood. Blockchain beyond bitcoin. Communications of the ACM, 2016; 59(11): 15–17.
83. Hadi Veisi, Reza Deihimfard, Alireza Shahmohammadi, and Yasoub Hydarzadeh. Application of the analytic hierarchy process (ahp) in a multi-criteria selection of agricultural irrigation systems. Agricultural Water Management, 2022; 267: 107619.
84. Ruchi Vishwakarma and Ankit Kumar Jain. A survey of ddos attacking techniques and defence mechanisms in the iot network. Telecommunication systems, 2020; 73(1): 3–25.
85. Jayneel Vora, Sudeep Tanwar, Sudhanshu Tyagi, Neeraj Kumar, and Joel JPC Rodrigues. Home-based exercise system for patients using iot enabled smart speaker. In 2017 IEEE 19th international conference on e-health networking, applications and services (Healthcom), 2017; pages 1–6. IEEE.
86. Marko Vukolic´. The quest for scalable blockchain fabric: Proof-of-work vs. bft replication. In Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers, pages 112–125. Springer, 2016.
87. Qin Wang, Bo Qin, Jiankun Hu, and Fu Xiao. Preserving transaction privacy in bitcoin. Future Generation Computer Systems, 2020; 107: 793–804.
88. Yujuan Wen, Fengyuan Lu, Yufei Liu, and Xinli Huang. Attacks and countermeasures on blockchains: A survey from layering perspective. Computer Networks, 2021; 191: 107978.
89. Xinyin Xiang and Xingwen Zhao. Blockchain-assisted searchable attribute-based encryption for e-health systems. Journal of Systems Architecture, 2022; 124: 102417.
90. Guangquan Xu, Hongpeng Bai, Jun Xing, Tao Luo, Neal N Xiong, Xiaochun Cheng, Shaoying Liu, and Xi Zheng. Sg-pbft: A secure and highly efficient distributed blockchain pbft consensus algorithm for intelligent internet of vehicles. Journal of Parallel and Distributed Computing, 2022; 164: 1–11.
91. Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, and Yousof Al-Hammadi. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, 2022; pages 1–16.
92. Sherali Zeadally and Oladayo Bello. Harnessing the power of internet of things based connectivity to improve healthcare. Internet of Things, 2021; 14: 100074.
93. Yu Zhan, Baocang Wang, Rongxing Lu, and Yong Yu. Drbft: Dele- gated randomization byzantine fault tolerance consensus protocol for blockchains. Information Sciences, 2021; 559: 8–21.
94. Fan Zhang, Ethan Cecchetti, Kyle Croman, Ari Juels, and Elaine Shi. Town crier: An authenticated data feed for smart contracts. In Proceedings of the 2016 aCM sIGSAC conference on computer and communications security, 2016; pages 270–282.
95. Guipeng Zhang, Zhenguo Yang, and Wenyin Liu. Blockchain-based pri- vacy preserving e-health system for healthcare data in cloud. Computer Networks, 2022; 203: 108586.
96. Tuo Zhang, Lei Gao, Chaoyang He, Mi Zhang, Bhaskar Krishnamachari, and A Salman Avestimehr. Federated learning for the internet of things: Applications, challenges, and opportunities. IEEE Internet of Things Magazine, 2022; 5(1): 24–29.
97. Zhenyong Zhang, Peng Cheng, Junfeng Wu, and Jiming Chen. Secure state estimation using hybrid homomorphic encryption scheme. IEEE Transactions on Control Systems Technology, 2020; 29(4): 1704–1720.
98. Zibin Zheng, Shaoan Xie, Hong-Ning Dai, Xiangping Chen, and Huaimin Wang. Blockchain challenges and opportunities: A survey. International journal of web and grid services, 2018; 14(4): 352–375.