Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

A Review on Blockchain technology in Healthcare application based secure Electronic Records Management

A. Ginavanee[1], Dr. S. Prasanna[2]
[1]Research Scholar, School of Computing Sciences VISTAS
[2]Professor and Head, Department of Computer Applications, VISTAS
ginainder@gmail.com prasanna.scs@velsuniv.ac.in

Abstract

Each medical service centre handles their own health records under the standard electronic health record (EHR) management system, which are difficult to transfer across various medical platforms. Blockchain technology has recently been one of the most popular options for allowing medical service centres based on various platforms to share EHRs. However, due to the size and cost of blockchain, it is difficult to keep all EHR data on it. Cloud computing is seen as a viable approach for resolving this issue. A thorough Systematic Literature Review was carried out to aid understanding of this distributed ledger technology, with goal of exploring recent literature on Blockchain in healthcare domain, identifying existing challenges and open questions and being guided by research questions about EHR in a Blockchain. The deep technical analysis looked at privacy, security, scalability, accessibility, cost, consensus techniques and type of blockchain utilised to evaluate articles. The SLR discovered that blockchain technology promised decentralisation, security, and privacy, all of which are commonly lacking in traditional EHRs. Furthermore, the outcomes of the extensive analyses would assist potential researchers with the type of blockchain to investigate in the future.

Keywords: electronic health record, Blockchain, healthcare, decentralization, security.

I. INTRODUCTION

Technology's recent advancements are touching many aspects of our life and altering how we use and view things. Technology is finding new methods to improve the healthcare sector, just as it has in other areas of life. The key advantages of technological innovation include enhanced security, user experience and other aspects of healthcare business. When employing this method, there were multiple opportunities to change and corrupt data. Healthcare databases, risk being permanently changed or erased, and data blocking is also a worry. A data blockage happens when medical data that should only be available to patients or hospitals is obtained by an unwanted entity such as a person. By tackling resource allocation and information blockade challenges, technology has the potential to enhance people's quality of life. It's all about timing when it comes to cloud-based healthcare data sharing [1]. Despite its popularity and varied options, cloud computing raises several privacy and security concerns. As a result, global enterprises have concentrated on building security rules as well as practises for cloud environment prior to employing it for business solutions. As a result, CSPs can no longer afford to lose their clients' trust in their outsourced data's security and privacy. In a cloud environment, its limitations make distributed and decentralised security solutions increasingly critical. By putting patient at centre of health system as well as boosting security, privacy and interoperability of health data, blockchain method has potential to revolutionise health care [2].

For diagnosis as well as treatment in healthcare, EHRs include crucial and extremely sensitive private information. An EHR is a digitally stored structure of a patient's health data that is developed as well as maintained throughout patient's life. It is often held by as well as distributed among different hospitals, clinics

and health providers. Patients often do not have simple access to historical data because these physicians have primary access to records. When patients gain access to their medical information, they engage with the data in a fragmented way, which reflects nature of how these records are administered. Due to the benefits it provides, including as improved security and cost effectiveness, EHR methods installed in a number of hospitals around world. They are considered an important aspect of the healthcare industry because they give a lot of functionality [3]. Electronic medical data storage, patient appointment administration, billing and accounts, and lab tests are among these features. They're included in a lot of the EHR systems utilised in the healthcare industry. The main goal is to deliver medical records that are safe, temper-proof, and shareable across multiple platforms. Despite fact that the goal of using EHR methods in hospitals or healthcare was to enhance quality of care, these methods had a number of issues and failed to reach the expectations [3]. In a study conducted in Finland to learn about nursing staff's experiences with EHRs, it was discovered that EHR systems had issues with reliability and user-friendliness [4]. Other issues that the EHR system encounters include the following:

Interoperability: It is a method for different data systems to communicate with one another. The data must be interchangeable and useable for further uses. HIE or data exchange in general, is a key feature of EHR systems. There are a variety of terminology, technical, and functional capabilities among the EHR systems used in different hospitals, hence there is no globally established standard [6]. Furthermore, the medical records being transmitted should be interpretable on a technological level, and the interpreted data could be used again [5].

Information Asymmetry: Information asymmetry, characterised by critics as one party having better access to information than the other, is currently the most serious problem in the healthcare business. This problem exists in EHR systems, as well as in the wider healthcare sector, because doctors and hospitals have access to patient records, making it central. Patients who want to examine their medical records must go through a long and inconvenient process. The data is only accessible to a particular healthcare entity, and only hospitals or organisations have control over it.

Data Breaches: Healthcare industry highlight necessity for a more robust structure. A study [6] analysed data breaches in EHR methods as well as found that since October 2009, 173 million data entries are compromised in these methods. Furthermore, numerous EHR methods are not built to meet demands as well as needs of patients, resulting in concerns such as inefficiency as well as poor method adaption. Literature also implies that usage of EHRs has had a negative impact on data processing. These issues make it reasonable to seek for a platform that can aid in transformation of healthcare sector to one that is more patient-centered, such as Blockchain [7].

A. Blockchain and its characteristics:

The data is stored on a blockchain, which is a decentralised node network. It's a great way to keep confidential data safe within the system. This technology aids in the secure and confidential communication of crucial data. It's a great way to keep all of your important documents in one place and secure. Utilizing a single patient database, blockchain also speeds up the search for applicants who meet certain trial conditions. The Blockchain is a decentralised P2P network of personal computers known as nodes that keeps track of, saves, and preserves history or transaction data [8]. It allows for reliable association because all network members can store and exchange information, and it keeps track of past as well as current experiences. This method can bring together diverse networks to reveal significance of individual therapy. As a result, Blockchain is well known for its immutability and security. The three fundamental concepts of Blockchain are blocks, nodes, and miners. None of the data on the blockchain is saved in a single location. Instead, Blockchain is copied as well as shared by a network of computers. Every computer connected to the internet updates its Blockchain to reflect a new block. Figure 1 depicts a high-level overview of blockchain technology.

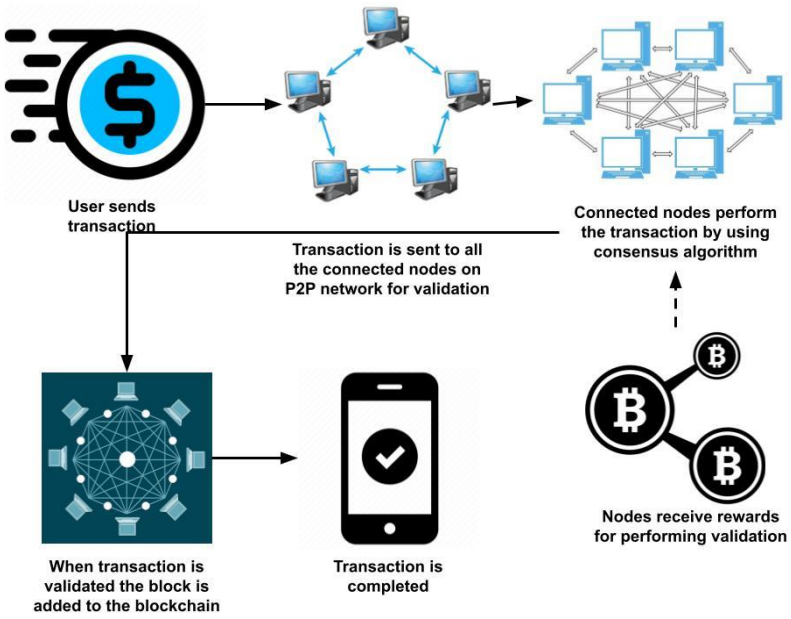

Fig. 1. An overview of blockchain architecture

A Blockchain system is based on internet and consists of a P2P network of computers that all run protocol as well as have an same copy of transaction log, allowing for P2P value transactions without necessity of an intermediary. Each Blockchain network has its own set of advantages as well as disadvantages that influence its potential applications. Public Blockchain was first implementation of Blockchain method was here that Bitcoin as well as other cryptocurrencies were born, and distributed ledger method was first advocated (DLT). It mitigates disadvantages of centralization, such as a lack of security as well as transparency. Rather of storing data in a single location, DLT disseminates data across a P2P network. Due to its decentralised nature, it necessitates some type of data verification [9].

- A private Blockchain network is one that works in a limited environment, such as a closed network, or is owned by a single entity. The creator of a private Blockchain network knows who participants are from outset. On the public web, permission-based solutions are impossible to create, and users are completely anonymous.

- Hybrid Blockchain, a type of Blockchain that integrates private as well as public Blockchain properties, is sometimes utilized by companies who want best of both worlds. It enables companies to create a private, permission-based method alongside a public, permissionless method, allowing them to control who has access to certain data kept on Blockchain as well as what data is made public.

B. Technical Characteristics of Blockchain-Based Systems

A distributed ledger method architecture is made up of several different technology components. More specifically, such systems make use of various data formats, distributed computing processes, and cryptographic algorithms combined with game theoretical notions. Message-passing mechanisms are used by clients to transact over a distributed P2P network. Each client's identification is recorded using a pair of public/private keys that are mathematically connected to each other in such a system. In reality, only a client's public key is visible to other network clients. Concept of a transaction [10] refers to the exchange of data between nodes. Concept of a transaction in a blockchain method can be generic and can contain any sort of data. Some blockchain protocols, for example, treat asset transfers as transactions. Each client who wants to engage with the

network signs the transaction using his or her private key. The signature transaction mechanism ensures transaction authentication and integrity across the whole network. The network then propagates the signed transactions, which must be validated before being added to underlying append-only structure. Before being appended to the ledger, all transactions are usually queued as well as their legitimacy is validated according to protocol's standards. All transactions are queued in transaction pool of Bitcoin blockchain, and miners propose blocks to be added to chain. Miners must verify I that each transaction is valid, and (ii) that current block refers to proper hash of prior block (every block is connected to preceding block's hash, establishing a chain, or the blockchain). If this is true, proposed block is added to chain, and all nodes are updated on current state of world. Method must maintain a global perspective of world among a group of untrustworthy parties that are competing with one another as well as attempting to reach a consensus, all while adhering to the norms and constraints laid forth in each protocol [11]. Bitcoin protocol, for example, proposes a computationally intensive consensus method for maintaining a level of robustness while incentivizing actors to participate in a computational race for validating blocks by solving a hash puzzle [12].

C. Need of blockchain in healthcare

In field of healthcare, pace of progress is enhancing at an astounding rate. Blockchain would be significant in revolutionising healthcare industry. Health-care environment is shifting toward a patient-centered method that emphasises two primary aspects: always-accessible services as well as suitable healthcare resources. Citizens can participate in health research studies utilizing Blockchain technology. Furthermore, better study and sharing data on public well-being would improve treatment for various groups. The entire healthcare system and organisations are managed using a centralised database [13]. Until date, the most serious problems in population health management data privacy, sharing, and interoperability. Data security is also a major concern, particularly in domains of personalised medicine as well as wearables. Figure 2 depicts the EHR's general blockchain architecture.

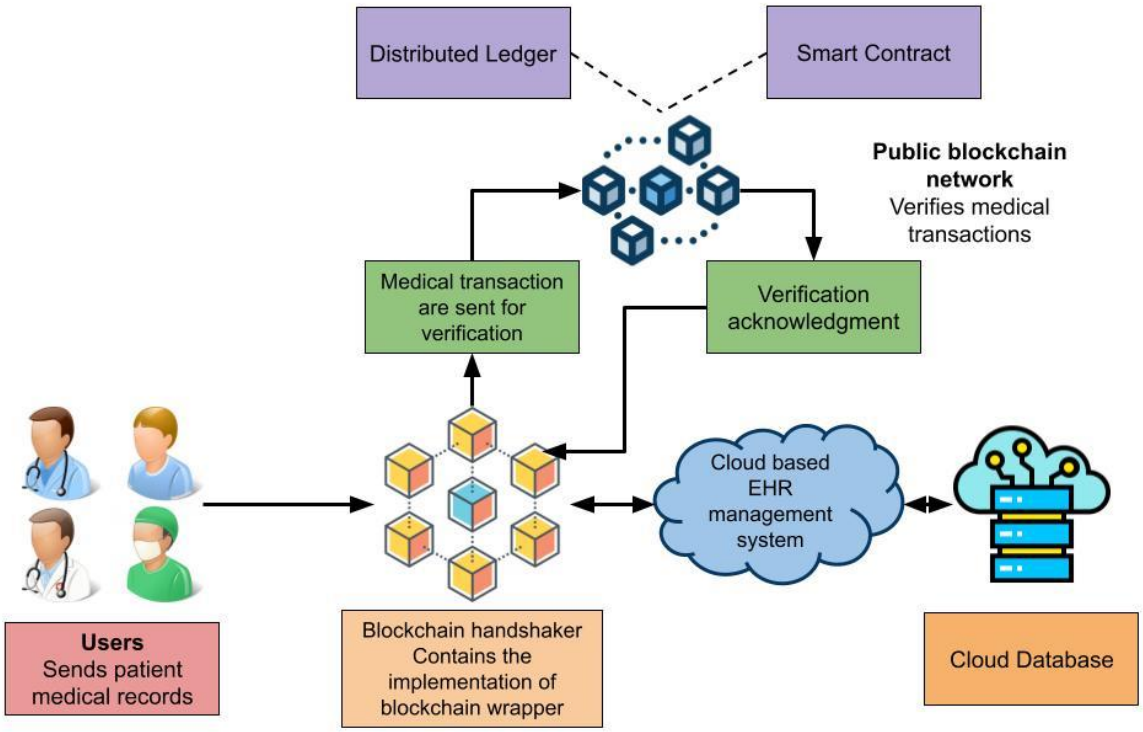

Fig.2. General blockchain architecture of EHR

D. Evolution of Blockchain:

As an emerging method, blockchain is transforming many industries, and its numerous benefits have opened up a slew of new study possibilities in a variety of fields; as a result, it has piqued the interest of research community. Rapid evolution of blockchain researches in recent years has necessitated the creation of research studies that examine current body of knowledge in this field in depth. The new global era has brought several changes to the way we use data. With the shift to digitization, social networks, smart phones, IoT (Internet of Things), analytics and cloud platforms are forming new ideas as well as intimate consumer relationships. New methods are being developed to change the integration of data as well as customer expectations so that better knowledgeable decisions can be made as well as user experience may be enhanced. With such a large volume of data in networks, ensuring security principles in a distributed context poses a significant issue. Satoshi Nakamoto first announced Blockchain as a Bitcoin Cryptocurrency [14], but it has evolved into much more. It provides a secure environment for the exchange of any service or transaction across a distributed network. As a result, it is transforming today's digital economy by adding new dimensions to system security as well as efficiency.

Blockchain technology has piqued the curiosity of a wide range of scholars as well as practitioners. Blockchain is a decentralised ledger that securely, verifiably, and transparently preserves all transactions done on top of a P2P network. Removal of a 3rd party can save processing costs while boosting transaction security as well as efficiency. The importance of Blockchain is compared to role of Internet in early 1990s due to the significant quantity of benefits it may provide to every business. Blockchain is transforming a variety of industries, including finance, IoT, healthcare, reputation systems, and supply chain management. As a result, in recent years, a significant amount of research undertaken in field of Blockchain. According to our data, Web of Science (WoS) has indexed over 1000 scientific papers in recent years. As number of research articles in Blockchain domain grows, there is a necessity for research studies that investigate a thorough overview of present body of knowledge in this topic [15].

BLOCKCHAIN 1.0: BITCOIN AND CRYPTOCURRENCY

Fundamentals of Bitcoin: The emergence of Blockchain described status of distributed ledger as a virtual coin, which is referred to as Bitcoin Blockchain. The money is called cryptocurrency because each coin has an electronic signature that uses the private key to sign transaction as well as public key to verify it. As a ledger record, each node in network stores a copy of this finite state transition method. The PoW was carried out with the help of the Bitcoin hashing scheme, which is based on HashCash as well as SHA-256 hash function. As a result, third parties were removed from a decentralised anonymous method in which a user may control his cash as well as conduct transactions [16].

BLOCKCHAIN 2.0: SMART CONTRACTS AND ETHEREUM

Beyond Bitcoin: Smart Contracts as well as Ethereum with move toward decentralisation, Bitcoin's restricted capabilities may no longer be sufficient for a general-purpose application. As a result, there was a need for a general-purpose development platform. Ethereum was introduced in 2013, and it addressed a number of problems with Bitcoin scripting. Smart Contracts, which are little computer programmes that exist and operate on blockchain, were made possible by Ethereum. The task is done independently and automatically, based on preset parameters for transaction validation. As a result, smart contracts lower cost of verification, arbitration, and fraud protection while also increasing transparency [17].

BLOCKCHAIN 3.0: CONVERGENCE TOWARDS DECENTRALIZED APPS

The existing technology cannot sustain the volume of micro-transactions that smart contracts are generating on a daily basis. Even if Ethereum's transaction rate improved to 15 tps from bitcoin's 7 tps, it is still insufficient to run today's economy. As a result, Blockchain is moving toward a decentralised internet that will include data

storage, communication networks, smart contracts, and open standards platforms. As a result, DApps (short for Decentralized Applications) are required. The backend of a DApp is hosted on a Blockchain Network, while the frontend code and user interface can be written in any programming language that can communicate with the backend. Decentralized storage platforms that support the frontend include Tangle, a mesh network that uses DirectAcyclic Graph(DAG) for validation [50]. As a result, the ultimate blockchain application is DApp hosted on a peer network, as it does not require any maintenance or governance, and thus does not require human intervention. This enables the creation of DAOs, in which all members share benefit by simply publishing their activity on Chain [18].

BLOCKCHAIN 4.0: SEAMLESS INTEGRATION WITH INDUSTRY 4.0.

We need an umbrella platform that can combine multiple services as well as architectures by permitting cross-chain connectivity, given the unbridled expansion of decentralised applications. The current Industry 4.0 guidelines call for an enterprise resource planning platform that can automate as well as integrate numerous execution platforms into a single cohesive entity. This necessitates an ever-increasing level of trust and anonymity, necessitating the creation of a scalable Blockchain network. To summarise, Blockchain 4.0 is a decentralised version of Blockchain 3.0 that may be used in real-world industrial and business logics to meet demands of Industry 4.0. Unibright [19], the first platform to support Industry 4.0, offers for a unified integration of blockchain business models. SEELE Platform is now facilitating cross-communication between various blockchain protocols across numerous services, bringing unity to the blockchain space. Individual chains within the complicated framework can harmonise their connections while operating independently. It uses a neural consensus technique that allows for linear scaling and can be used on-chain and off-chain. It also allows for transactional speeds of up to 1 million transactions per second (TPS), which is now unthinkable in a public blockchain [20].

E. Classification of Block chain:

Blockchain technology is a decentralised platform that allows members in a P2P network to share data. Partially decentralised and fully decentralised blockchains are classed based on their architectural traits as well as quality criteria. Consensus method, smart contract, transaction capacity, forks, absence of authorization, and lack of fees, the platforms are compared [21].

TABLE I. Comparison table of blockchain platforms

	Bitcoin [11,13]	**Ethereum [16]**	**Hyperledger Fabric [17]**	**Hyperledger Burrow [18]**	**Ripple [19]**
Blockchain-Type	Public	Public / Private	Private / Consortium	Private / Consortium	Private
Consensus	PoW	PoW/PoS	PBFT	Tendermint	BFT(RPCA)
Smart contract	No	Yes	Yes	Yes	Yes
Capacity	7 tps	12 tps	Thousands tps	Thousands tps	Thousands tps
Forks	Yes	Yes	No	No	No
Permission-less	Yes	Yes/No	No	No	No
Fee-less	No	No	Yes	Yes	No

Permission-Less Blockchain (Public Blockchain)

There are no restrictions on anyone joining blockchain network in a permission-less or public blockchain, and they can participate in transaction validation and mining. Every peer in a public blockchain network has complete permissions to participate in transaction validation and block ledger maintenance processes. PoW is one of the greatest solutions for public blockchain difficulties such avoiding data modification, however this consensus requires 51 percent of participants or miners to run network [22].

Permissioned Blockchain

Permissioned blockchains are polar opposite of public blockchains in that they are closed networks where every peer is approved by organisation before joining. Authenticated players govern mining method of permissioned blockchains. It employs P2P technology to alert participants of block transactions. A public blockchain requires currency or tokens for transaction processing, whereas a private blockchain does not. Hyperledger Fabric as well as Ripple are two examples of private blockchain platforms. All participants in the permissioned blockchain are recognised in Hyperledger Fabric, and they reach a consensus using the PBFT mechanism. PBFT is permissioned blockchains' consensus techniques, allowing only permissioned peers to participate in the network's transaction validation process. Ripple also uses BFT, which is adapted in RPCA [23], to establish a consensus process.

Consortium Blockchain (Hybrid Blockchain)

It is a hybrid of private as well as public blockchains in which consensus processes are governed by a group of organisations or participants in order to assure transaction validation. Finally, the permission-less blockchain necessitates large computations to add new blocks to network. As a result, it is unsuitable for IoT devices with limited resources. As a result of their low latency and high transaction volume, private as well as consortium blockchains are more suited for IoT [24].

Mining in blockchain technology:

The computational labour that nodes in blockchain network do in aim of earning additional tokens is referred to as "mine." In reality, miners are being compensated for acting as auditors. They are in charge of ensuring the legitimacy of Bitcoin transactions. Bitcoin mining is method of putting new bitcoins into circulation. It's also how blockchain's network confirms new transactions, and it's a crucial aspect of its care and development. Mining is carried out using high-tech hardware to solve a tough computational arithmetic problem. When first machine solves issue as well as obtains next block of bitcoins, the process is restarted. Mining cryptocurrency is time-consuming, costly, and rarely rewarding. Many cryptocurrency investors, on the other hand, are drawn to mining since miners are paid with crypto tokens in exchange for their work. This could be because, like California gold prospectors in 1849 [25], businesspeople saw mining as a divine gift.

Consensus algorithm:

This section will wrap up various terminology that were supplied without much explanation in the preceding sections, such as the nonce field and PoW, which is a proposal for adding a new block to chain. Furthermore, main focus of this section is on how nodes in verifying network agree on the ledger they each have. The proof-based consensus method as well as vote-based consensus method are two main subsections of this section.

Proof-Based Consensus method

For nearly three decades, consensus procedures in distributed methods are well-studied research subject. These procedures allow a group of dispersed nodes to reach an agreement on a common state or data. Because of need for a shared state, replicated database systems were developed to enable network resilience against node

failures. The concept of State Machine Replication (SMR) [26] can be used to generalise the concept of a replicated database. A computing machine is described as a deterministic state machine, which is underlying principle underpinning SMR. The machine receives an input message, conducts the predetermined computation, and may output/respond. These activities basically alter the state of the object. According to SMR, a state machine with an initial state is duplicated across multiple nodes. If all of participating nodes receive same set of input messages in exact same order, then each node's state machine can evolve in the same way. Even in case of node failures, this can provide consistency as well as availability regarding state of machine (as well as the data it carries) across all (suitable) nodes. When this happens, participating nodes are considered to have reached a distributed consensus. A protocol must be specified to enable timely dissemination as well as atomic broadcast of input messages among nodes, and it also specifies how a distributed consensus is formed as well as maintained in many ways. As a result, such a protocol is appropriately referred to as a consensus protocol. Designing as well as deploying a consensus protocol is a difficult process since it must take into account a number of important factors such as node robustness, node behaviour, and so on [27]. Schneider emphasised that there are two critical prerequisites for achieving and maintaining distributed node consensus. A deterministic state machine is the first requirement. The second requirement is a consensus protocol for disseminating inputs quickly and ensuring atomic broadcast across participating nodes. Making specific assumptions under which protocol is proven to work properly is one technique to meet the design goals of such a protocol. The critical aspects of a consensus protocol are influenced by these assumptions. Following that, we look at two sets of assumptions that are commonly employed in distributed consensus protocols.

Proof-Based Consensus Method

It is described in this section. PoW [28], proposed by Nakamoto, is the original work. Many proof-based consensus methods are presented to date, including those based on PoW, PoS, their hybrid version, and other variants developed independently of these two major ones. Essential premise of a proof-based consensus method is that among many nodes joining network, node that performs adequate proof will be given authority to append a new block to chain as well as rewarded [29].

PoW-based consensus algorithm

POW used in article "Bitcoin: A Peer-to-Peer Electronic Cash System" is proof of workload. On basis of decentralisation, the pow consensus method is utilized to overcome problem of node trust. Issue is that the blockchain can achieve a balance between a large number of nodes. Blockchain addresses challenge of sending trusted data as well as transferring value via untrusted channels, and consensus methods. Problem of consistency has provided groundwork for Bitcoin system's security. POW technique is used by Bitcoin to generate blocks. It takes a lot of trial calculations to acquire a good Block Hash, and calculation time is dependent on machine's hash speed. When a node has n percent of network's computational power, it has a n/100 chance of discovering Block Hash. Other users have verified as well as authorised the block. The user can receive matching reward after adding to main chain. A block is represented here as a packet comprising triples B =, where h' is previous block's hash and txs is block's transaction record. A 32-bit integer is Nonce. For current block hash value, D specifies how many leading zeros are required. The higher the number of leading 0s, the more complex it is. There is no way to foresee which kind of nonce will match needs because changing any bit in the nonce will totally modify hash H(B). To achieve block requirements, the node must employ its computer capabilities to try a large number of different nonce values so that H(B) D [30]. Following is procedure for integrating consensus method into digital money method:

1) New transaction is broadcast to all miners on network.
2) Each miner gathers transaction data as well as builds a Merkle tree.
3) Miner use computing resources to locate a nonce that is compatible with present difficulty level.
4) Miner comes up with a workable nonce solution as well as transmits block to entire network.
5) Block is verified by other miners.

6) If transaction record in this block is authentic, block hash fulfils struggle value condition, other honest nodes produce next block.

Advantage:

1. Decentralization is high: method is simple as well as straightforward to execute, nodes can freely enter and degree of decentralisation is high.

2. High security: Impairment to method necessitates a significant financial commitment, and security is highly high.

3. Machine trust: Node solving hash function solves problem of choosing block producers. The generation and verification of suggestion to consensus is a completely mathematical task in end. Without exchanging any further information, the nodes can achieve a consensus. The entire procedure There is no need for human intervention.

Disadvantages:

1. Long confirmation time: The confirmation time of block is difficult to reduce in order to maintain the degree of decentralisation.

2. poor expansion: The lack of finality necessitates the use of a checkpoint mechanism to compensate, yet the likelihood of obtaining consensus has increased exponentially as the number of validations has improved.

3, waste of resources: Due to difficulty of mining and need to replace hardware, there is a twofold waste of hardware and resources.

POS: Due to the blockchain's unique data structure, the consensus process may be viewed as a leader election mechanism in which a fixed system selects a leader (booking miner) at random, and that individual releases a new block, avoiding a single confirmation. For a long period, the ledger is under the control of the user or group. However, as the blockchain grows in popularity, we can observe that the current proof technique has a number of flaws. To begin with, bitcoin network uses a lot of energy. To save resources, several mines are built near to hydropower plants. This concept is also derived from economic society. Higher dividends as well as dividends a person receives, more shares he owns. No additional resource usage is necessary if the blockchain can be maintained in this state. It has the potential to create natural inflation in blockchain assets. This sounds excellent and has characteristics that are similar to those of physical currency. Difficulty of mining miners in blockchain can be affected by these assets. More assets you have, more organic accounting you'll need. Determine the nonce that satisfies the criteria. As a result, the hashing problem we must solve is: target age of proofhash coins. You can think about POS in this way: similar to a bank account, this method will assign you appropriate interest based on amount as well as duration of digital money you own. Simply explained, it's a method that pays you interest based on how much money you have and how long you've had it. If you store 100 coins for a total of 30 days, your currency will be 3000. Money is fascinating, and there is a rate of interest on currency [31].

Advantage:

1. Save resources: The currency is in an interest-bearing manner, and mining does not waste electricity.

2. Block confirmation time is fast: Because node mining does not involve physical evaluations as well as just requires equity verification, pos consensus enhances block confirmation efficiency. This drastically minimizes time for consensus validation.

Disadvantages:

1. Poor security: Execution rules are complicated, there are a lot of intermediary procedures, and there are a lot of human elements involved, thus it's easy to find security flaws.
2. pointcheck: There is no finality, like with the POW consensus process, and a checkpoint mechanism is required to compensate.
3. Matthew effect: Under the POS consensus process, the total quantity of equity is multiplied by number of coins at time of having currency. It will almost certainly result in a winner.
4. Accounting node incentive issue: Mining in pos does not waste power expenditures; yet, while PoS mining has a confident incentive, it is quite limited in comparison to pow mining.
5. Nothing-at-Stake attack: Because mining is free, the success rate of fork attacks is very high. You can start a fork attack even if you don't have 51 percent interest.

DPOS: Delegated proof of stake

DPos works in a comparable way to a board vote in that it allows holder to cast a set number of nodes as well as have them proxied for verification as well as accounting. BitShares community was the first to propose DPOS consensus. It differs from POS consensus in that node elects numerous agents, each of whom is confirmed and billed by the agent. When compared to POS, DPOS can significantly improve election efficiency, albeit at the sacrifice of several decentralisation benefits. Witnesses, delegates, and employees are the three sorts of people who can vote in Bitshares consensus method. Witnesses are compensated for processing transactions as well as keeping blockchains. Representative will not be compensated, but he will be able to suggest that Bitshare be updated. Workers can suggest projects, and if the project is approved, they will be paid. The witness election procedure and the witness block are both part of the DPOS consensus process. The witness's role is limited to witnessing transaction, validating signature as well as time stamp, and refraining from participating in it. Each network account has ability to vote for its own witness. You get more votes if you hold more blockchain assets [32].

1) Witness Election permanent node with voting rights accepts vote as well as top N witnesses are eventually chosen. At regular periods, list of witnesses is rotated.

2) Witnesses have been summoned from all corners of city. Witnesses are compensated for every block they yield as well as their pay is based on the number of votes they obtain. If witness are unable to earn a living as well as may be voted to lose their identity. DPOS consensus process is simple and efficient since it does not require mining or complete node verification. Instead, it is validated by a small number of witness nodes. DPOS consensus questioned too centrally because to the low number of verification nodes. Find of blocker known for a long time, making collusion assaults more feasible. The DPOS algorithm is more centralised than the first two consensus techniques.

Advantage:

1. Simple and efficient: To establish a second-level consensus verification, significantly minimize number of participating verification as well as accounting nodes.
2. Save resources: Only primary node is required to verify network.
3. High scalability: 2nd level verification, quick block-out, and high main network capacity
4. Disadvantages: Tokens are used throughout the consensus system, although numerous commercial applications do not need them.

Disadvantages:

1. Centralization: Excessive centralization is being avoided by lowering the number of verification nodes, rather than universal. This is a departure from basic spirit of everyone in blockchain world.
2. Bribery makes main network fail: Inability to finish main network vote, as well as super-node bribery, have all contributed to eos governance becoming perplexing.

PBFT: Practical Byzantine Fault Tolerance

The service is designed as a state machine as well as executes replica replication at multiple nodes of distributed method. A replica of every state machine saves service's state and also implements service's functionality. An uppercase letter R represents a collection of all copies, as well as every copy is indicated by an integer. Assume |R|=3f+1 for sake of simplicity. The following method governs the operation of the entire algorithm. In a distributed system, there are 3f + 1 nodes that can tolerate f Byzantine error nodes [33].

1) Client asks primary node's calling service.
2) Request is multicast to secondary node by master node.
3) Request is executed as well as response is sent to the client by the secondary node.

4) The client receives f + 1 identical responses, and client receives desired data. Because Byzantine fault-tolerant method requires advance knowledge of the number of nodes, nodes cannot create connections with one another, and nodes cannot be dynamically managed, preventing public chain from meeting its requirements. However, such as China Central Bank's electronic billing method, Hyperledger Fabric, where the number of nodes is fixed, PBFT algorithm can be used to reach blockchain consensus. The primary network is stable without a fork, which is an advantage.

Disadvantages:

1. The breadth of application is limited: only alliance chains and private chains are supported.
2.Poor scalability.
3. Node is fixed: it cannot cope with public chain's open environment; it only smears to alliance chains or private chains.
4. Low fault tolerance: Total number of nodes needed by PBFT algorithm is n>=3f+1. Number of failed system nodes should not exceed 1/3 of total network nodes, and fault tolerance rate should be low.

We analyse blockchain common chain as well as licence chain consensus algorithms, as well as the benefits as well as drawbacks of each algorithm in terms of resource consumption, centralization degree as well as transaction validation time [34].

TABLE II. Advantages and disadvantages of each method

Consensus protocols	**Advantage**	**Disadvantages**
Pow	1.Safe and stable, high degree of freedom of nodes 2.High degree of decentralization, open node system	1.Weak scalability and low performance 2.Causing hardware equipment waste
Pos	1.Less energy 2.High degree of decentralization, open node system	implementation process 2.Security breach
Dpos	1.Less energy 2.High performance 3.Finality	1. Weak degree of decentralization, closed node system
Pbft	1.Higher performance 2.Finality 3.High security	1. Weak degree of decentralization, closed node system 2. low fault tolerance

Comparison between different blockchain techniques:

The literature on blockchain was analysed and split into several areas, including consensus mechanisms, smart contracts, IoT, healthcare, business, and numerous blockchain platforms. Similarly, review papers relating to IoT, business, and healthcare are summarised in the top-right Venn diagram. A few studies [35] deal with both IoT and corporate applications. Based on our analysis, we can confidently conclude that the majority of review articles to far have focused on exploring blockchain method for a certain application area. There are, however, a few recent studies that focus on a variety of application areas. The potential benefits of blockchain in many industries, supply chain management, accounting settlement, and smart trading, for example, are briefly examined in [36]. Similarly, the needs for blockchain application in many areas, such as financial [38], healthcare, logistics, manufacturing, energy, and robotics, were evaluated in [37]. We give a comprehensive analysis of existing blockchain applications in wide areas of IoT, Business, and Healthcare, as well as their difficulties in this post. We also take a close look at existing blockchain basic structures. In conclusion, in a single draught, this article offers reader with an understanding of key architectures as well as three broad application areas of blockchain method.

Several recent research [39] have established the basic blockchain technology components that facilitate healthcare applications, such as hash-chain timestamping and consensus techniques like PoW. There are three ways for dealing with the scalability problem: the Merkle tree, lightweight nodes, and unspent transaction output. As a distributed network, blockchain confronts various difficulties, such as the synchronisation difficulty known as the Byzantine Generals' Problem. The Hyperledger platform is being proposed by an oncology clinical data sharing framework10 for patient care [40]. ModelChain's use of blockchain allows diverse institutions to enhance prediction power by adding data to a collaboratively produced method without having to send data or method to a central location. ModelChain's first deployment was for predictive analytics in anaesthesia, and it employed a permissioned blockchain called MultiChain. These examples are preliminary in nature and are intended to demonstrate the viability of using popular, open-source blockchain systems for health and medicine. Some health-related blockchain apps, such as Luna DNA, a proposed genomic as well as medical research database, do not clearly identify their underlying platforms [41].

Ethereum. For patient-managed health data exchange apps, MedRec and Patientory propose using a blockchain based on Ethereum platform. Nebula Genomics proposes utilizing an Ethereum-based blockchain platform to share and analyse genetic data. Ethereum suggested for use in clinical applications like clinical data exchange as well as automated remote patient monitoring.

In recent years, experts have concentrated on proposing blockchain method as a secure option for online data exchange between participants in healthcare industry. In a white paper issued by [42], for example, the authors proposed a novel distributed blockchain infrastructure for allowing the integration as well as secure interoperability of healthcare data across a wide range of stakeholders around world. Their key motive for writing this study is a lack of common architecture as well as standards for efficient and secure transmission of healthcare data. Before using blockchain method in healthcare field, they recommend checking for the four preconditions in the first phase. In the event that these circumstances are met, they recommend using blockchain. They recommend that healthcare organisations build use cases primarily to validate as well as authenticate data or the value of transactions involved in use case in the second phase. Smart contract, which executes automatically when certain circumstances are met, is discussed in the third phase. This strengthens the technology by increasing stakeholder trust. In the final phase, the proposed blockchain system will be implemented as either a permissioned or permissionless blockchain. In a transaction layer, they also describe concepts of on-chain as well as off-chain data. Authors of [43] proposed a blockchain-based solution to health data interchange. They address the issue of healthcare data sharing and interchange across institutions. This is a huge issue in the healthcare industry, owing to privacy issues and regulations. They establish the form and semantics of the block holding patient registrations in the healthcare blockchain after first defining various assumptions relating to the parties involved. Then, similar to Bitcoin, they establish four processes for adding a new block to blockchain. As a hashing algorithm, they employ SHA 256. Then they propose a proof-of-

interoperability algorithm for network consensus. For exchanging health records, FHIR [44] standard is utilized. Pending transactions, a list of FHIR profile URLs, the current block, and a list of valid transactions are all inputs to the proposed method. It first verifies profile conformance, then sends a validate request to the FHIR server, and then verifies the answer for interoperability proof. In [45], the authors developed a strategy for ensuring patient data privacy on a private blockchain. On a private blockchain network, they propose using a privacy-preserving online ML algorithm like explorer. Each bock represents a transaction, which consists of the following elements: model, flag, hash, and error. Authors next offer a method for information proof. The method takes into account the shareholder site S, the waiting and polling time periods, and the number of sites N involved in transaction. Technique generates [46] model, which is the most recent online ML model.

Table 3. Blockchain solutions for healthcare

Contribution from research community				
Author referred	**Problem addressed**	**Major contribution**	**Strength and weakness**	**Year**
Delolite [12]	Interoperability of health care information	Proposed distributed blockchain framework for secure info exchange	Increase trust by smart contract parties needs to trust	2016
Peterson [138]	Secure health info exchange limited access to healthcare info	Health information exchange blockchain model	Use FHIR for proof of interoperability	2016
Tsung [140]	Ensure privacy	Privacy preserving online machine learning algorithm	Each block has flag, hash and error	2018
Iyengar [148]	Access control	Cloud based healthcare system	Requirement of cloud app with strict privacy	2018
Zhang [149]	Interoperability of healthcare information	Apply software pattern for interoperability in blockchain healthcare	Discuss implementation challenges	2017
Leo [136]	Challenges to adoption of blockchain for healthcare	Blockchain uses in healthcare and complex challenges	Benefits and adoption challenges presented well	2018
Contribution from industry				
Author referred	**Problem addressed**	**Major contribution**	**Strength and weakness**	**Year**
Tieron [16]	Verification of medical records	Foresee blockchain for verification of range of things	product	2015
Proof [141]	Integrity of healthcare data	Use bitcoin block chain to prove integrity and timestamp data	Product	2016
Gartner [150]	privacy	Number of projects	Projects	2016

		to use of blockchain techniligy		
Gem [17]	Secure sharing and access control	GEMOS	Product	2017
Blockchain health [147]	Interoperability	Secure connect between stakeholder to share health research	Research projects and product	2016
GitHub [2]	Interoperability	Projects related to using blockchain in healthcare	Projects	2017

II. CONCLUSION

Because of its inherent encryption and decentralisation, Blockchain has a number of unique applications in healthcare. It improves the security of patients' EMRs, encourages monetisation of health data, increases interoperability between healthcare organisations as well as aids in the fight against counterfeit drugs. Blockchain technology has the potential to alter various healthcare fields; in domains like healthcare, digital agreements enabled by intelligent contracts are one of Blockchain's most important uses. Blockchain's potential in healthcare depends on adoption of linked advanced methodologies in ecosystem. It includes system tracking, healthcare insurance, medicine tracking, and clinical studies. Hospitals can use a Blockchain framework to track their services over their whole life cycle, employing device tracking. Blockchain method has potential to improve patient history management, particularly tracking. Overall, this method would improve healthcare services by dramatically enhancing as well as eventually revolutionising how patients as well as clinicians treat as well as use clinical records.

REFERENCES

[1] S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain technology in healthcare: a comprehensive review and directions for future research, Appl. Sci. 9 (9) (2019) 1736.
[2] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, M. Ylianttila, Blockchain utilisation in healthcare: key requirements and challenges, in: In2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom), IEEE, 2018 Sep 17, pp. 1–7.
[3] G. Moona, M. Jewariya, R. Sharma, Relevance of dimensional metrology in manufacturing industries, MAPAN 34 (2019) 97–104.
[4] M.H. Kassab, J. DeFranco, T. Malas, Giuseppe Destefanis Laplante, V.V. Neto, Exploring research in Blockchain for healthcare and a roadmap for the future, IEEE Trans. Emerg. Top. Comput. (2019), 1-1.
[5] B. Shen, J. Guo, Y. Yang, MedChain: efficient healthcare data sharing via Blockchain, Appl. Sci. 9 (6) (2019) 1207.
[6] U. Chelladurai, S. Pandian, A novel blockchain based electronic health record automation system for healthcare, J. Ambient Intell. Humanized Comput. (2021).
[7] P. Zhang, D.C. Schmidt, J. White, G. Lenz, Blockchain technology use cases in healthcare, in: Advances in Computers, vol. 111, Elsevier, 2018 Jan 1, pp. 1–41.
[8] I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, Blockchain for healthcare data management: opportunities, challenges, and future recommendations, Neural Comput. Appl. (2021 Jan 7) 1–6.
[9] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, ‘‘Blockchain technology in healthcare: A systematic review,’’ Healthcare, vol. 7, no. 2, p. 56, Apr. 2019.
[10] E. Chukwu and L. Garg, ‘‘A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations,’’ IEEE Access, vol. 8, pp. 21196–21214, 2020.

[11] S. Khezr, A. Yassine, and R. Benlamri, ‘‘Blockchain technology in healthcare: A comprehensive review and directions for future research,’’ Appl. Sci., vol. 9, no. 9, p. 1736, 2019.
[12] I. Ahmed, M. Ahmad, G. Jeon, and F. Piccialli, ‘‘A framework for pandemic prediction using big data analytics,’’ Big Data Res., vol. 25, Jul. 2021, Art. no. 100190.
[13] R. Vaishya, M. Javaid, I. H. Khan, and A. Haleem, ‘‘Artificial intelligence (AI) applications for COVID-19 pandemic,’’ Diabetes Metabolic Syndrome: Clin. Res. Rev., vol. 14, no. 4, pp. 337–339, Jul. 2020.
[14] L. Houston, Y. Probst, and A. Humphries, ‘‘Measuring data quality through a source data verification audit in a clinical research setting,’’ Stud. Health Technol. Inform., vol. 214, pp. 13–107, Jan. 2015.
[15] M. Muthuppalaniappan and K. Stevenson, ‘‘Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health,’’ Int. J. Qual. Health Care, vol. 33, no. 1, Feb. 2021.
[16] M. S. Rahman, I. Khalil, P. C. Mahawaga Arachchige, A. Bouras, and X. Yi, ‘‘A novel architecture for tamper proof electronic health record management system using blockchain wrapper,’’ in Proc. ACM Int. Symp. Blockchain Secure Crit. Infrastruct. (BSCI), 2019, pp. 97–105.
[17] H. Wu, Y. Shang, L. Wang, L. Shi, K. Jiang, and J. Dong, ‘‘A patient-centric interoperable framework for health information exchange via blockchain,’’ in Proc. 2nd Int. Conf. Blockchain Technol. Appl., Dec. 2019, pp. 76–80
[18] S. Wu and J. Du, ‘‘Electronic medical record security sharing model based on blockchain,’’ in Proc. 3rd Int. Conf. Cryptogr., Secur. Privacy (ICCSP), 2019, pp. 13–17.
[19] A. Fernandes, V. Rocha, A. F. D. Conceicao, and F. Horita, ‘‘Scalable architecture for sharing EHR using the hyperledger blockchain,’’ in Proc. IEEE Int. Conf. Softw. Archit. Companion (ICSA-C), Mar. 2020, pp. 130–138.
[20] A. A. Mamun, A. Al Mamun, S. R. Hasan, S. R. Hasan, M. S. Bhuiyan, M. S. Bhuiyan, M. S. Kaiser, M. S. Kaiser, M. Abu Yousuf, and M. A. Yousuf, ‘‘Secure and transparent KYC for banking system using IPFS and blockchain technology,’’ in Proc. IEEE Region 10 Symp. (TENSYMP), 2020, pp. 348–351.
[21] A. Zhang and X. Lin, ‘‘Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain,’’ J. Med. Syst., vol. 42, no. 8, p. 140, 2018.
[22] T. T. Thwin and S. Vasupongayya, ‘‘Blockchain-based access control model to preserve privacy for personal health record systems,’’ Secur. Commun. Netw., vol. 2019, pp. 1–15, Jun. 2019.
[23] T. Zhou, X. Li, and H. Zhao, ‘‘Med-PPPHIS: Blockchain-based personal healthcare information system for national physique monitoring and scientific exercise guiding,’’ J. Med. Syst., vol. 43, no. 9, p. 305, Sep. 2019.
[24] R. Jabbar, N. Fetais, M. Krichen, and K. Barkaoui, ‘‘Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity,’’ in Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT), Feb. 2020, pp. 310–317.
[25] Y. Zhuang, L. R. Sheets, Y.-W. Chen, Z.-Y. Shae, J. J. P. Tsai, and C.-R. Shyu, ‘‘A patient-centric health information exchange framework using blockchain technology,’’ IEEE J. Biomed. Health Informat., vol. 24, no. 8, pp. 2169–2176, Aug. 2020.
[26] O. Gutiérrez, G. Romero, L. Pérez, A. Salazar, M. Charris, and P. Wightman, ‘‘HealthyBlock: Blockchain-based IT architecture for electronic medical records resilient to connectivity failures,’’ Int. J. Environ. Res. Public Health, vol. 17, no. 19, p. 7132, Sep. 2020.
[27] P. Meier, J. H. Beinke, C. Fitte, and F. Teuteberg, ‘‘Generating design knowledge for blockchain-based access control to personal health records,’’ Inf. Syst. e-Bus. Manage., vol. 19, pp. 13–41, Aug. 2020.
[28] R. Kumar and R. Tripathi, ‘‘Secure healthcare framework using blockchain and public key cryptography,’’ in Blockchain Cybersecurity, Trust Privacy. Cham, Switzerland: Springer, 2020, pp. 185–202.
[29] T. T. Thwin and S. Vasupongayya, ‘‘Performance analysis of blockchainbased access control model for personal health record system with architectural modelling and simulation,’’ Int. J. Netw. Distrib. Comput., vol. 8, no. 3, p. 139, 2020.
[30] L. Ismail, H. Materwala, and M. A. Khan, ‘‘Performance evaluation of a patient-centric blockchain-based healthcare records management framework,’’ in Proc. 2nd Int. Electron. Commun. Conf., Jul. 2020, pp. 39–50.

[31] L. Ismail and H. Materwala, ‘‘BlockHR: A blockchain-based framework for health records management,’’ in Proc. 12th Int. Conf. Comput. Modeling Simulation, 2020, pp. 164–168.
[32] Z. Li and L. Zhang, ‘‘An EMR sharing and privacy protection mechanism based on medical consortium blockchain,’’ in Proc. 6th Int. Conf. Comput. Technol. Appl., Apr. 2020, pp. 160–164.
[33] X. Yang, T. Li, W. Xi, A. Chen, and C. Wang, ‘‘A blockchain-assisted verifiable outsourced attribute-based signcryption scheme for EHRs sharing in the cloud,’’ IEEE Access, vol. 8, pp. 170713–170731, 2020.
[34] M. Al Baqari and E. Barka, ‘‘Biometric-based blockchain EHR system (BBEHR),’’ in Proc. Int. Wireless Commun. Mobile Comput. (IWCMC), Jun. 2020, pp. 2228–2234.
[35] S. Ali, G. Wang, B. White and R. L. Cottrell, A Blockchain-Based Decentralized Data Storage and Access Framework for PingER, (2018)
[36] E. Zaghloul, T. Li, M. Mutka and J. Ren, d-MABE: Distributed Multilevel Attribute-Based EMR Management and Applications, (2020)
[37] TechSci Research, Global Electronic Health Records (EHR) Market (2020 to 2025), (2020)
[38] Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K, Security Aspects of Blockchain Technology Intended for Industrial Applications, (2021)
[39] M. Chen, Y. Qian, M. Chen, K. Hwang, S. Mao, and L. Hu, “Privacy protection and intrusion avoidance for cloudletbased medical data sharing,” IEEE Transactions on Cloud Computing, vol. 8, no. 4, pp. 1274–1283, 2020
[40] M. Mustafa and S. Alzubi, “Factors affecting the success of Internet of things for enhancing quality and efficiency implementation in hospitals sector in Jordan during the crises of Covid-19,” in Internet of Medical Things for Smart Healthcare. Studies in Big Data, C. Chakraborty, A. Banerjee, L. Garg, and J. J. P. C. Rodrigues, Eds., vol. 80, Springer, Singapore, 2020.
[41] R. Ranjan and S. Shekhar, “Securing healthcare data with healthcare cloud and blockchain,” in Emerging Technologies in Data Mining and Information Security, pp. 439–456, Springer, Singapore, 2021.
[42] S. Sharma, A. Mishra, and D. Singhai, “Secure cloud storage architecture for digital medical record in cloud environment using blockchain,” in Proceedings of the International Conference on Innovative Computing & Communications (ICICC) 2020, 2020.
[43] B. Shen, J. Guo, and Y. Yang, “MedChain: efficient healthcare data sharing via blockchain,” Applied Sciences, vol. 9, no. 6, p. 1207, 2019.
[44] J. Qu, “Blockchain in medical informatics,” Journal of Industrial Information Integration, vol. 25, article 100258, 2022.
[45] F. A. Reegu, S. M. Daud, S. Alam, and M. Shuaib, BlockchainBased Electronic Health Record System for Efficient Covid-19 Pandemic Management, preprints.org, 2021.
[46] J. A. Santos, P. R. M. Inácio, and B. M. Silva, “Towards the use of blockchain in mobile health services and applications,” Journal of Medical Systems, vol. 45, no. 2, pp. 1–10, 2021.