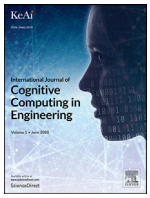
International Journal of Cognitive Computing in Engineering 4 (2023) 220–239

Contents lists available at ScienceDirect

International Journal of Cognitive Computing in Engineering

journal homepage: https://www.keaipublishing.com/en/journals/international-journal-of-cognitive-computing-in-engineering/



Amalgamation of Blockchain with resource-constrained IoT devices for healthcare applications – State of art, challenges and future directions

Pawan Hegde, Praveen Kumar Reddy Maddikunta*

School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India

ARTICLE INFO

Keywords:
Blockchain
Internet of Things (IoT)
Healthcare, Medical services
Blockchain IoT integration
Resource-constrained

ABSTRACT

Healthcare is an emerging sector with the integration of emerging technologies aiming to improve Quality of Life of an individual through various medical services. Most of the healthcare services work with sensitive information of patients either collected in real-time using body implanted sensors or through various IoT enabled medical devices during the diagnosis in a centrally controlled model. But, the traditional IoT based medical services suffer from several challenges such as data security, privacy, interoperability, single point of failure, scalability, and data integrity. However, by considering the advantages of Blockchain technology and the disadvantages of IoT systems, the amalgamation of a decentralised, distributed ledger technology with the IoT for various healthcare applications will strengthen the system by resolving the major challenges. Thus, this research article conducts a comprehensive survey on the integration of Blockchain and IoT (BCIoT) for Healthcare services, focusing mainly on existing approaches, possibilities, applications and challenges. First, we present a detailed overview of Blockchain, IoT and the motivation for BCIoT along with the survey on existing healthcare applications. Next we discuss the enabling platforms for BCIoT based healthcare services. For the better understanding, we review the role of BCIoT in Remote patient monitoring, electronic heath record management, Health asset tracing, Covid-19 infected patient contact tracking. Finally challenges and future directions are discussed to improve the Quality of Life of patients through Healthcare applications.

1. Introduction

Recent year's healthcare industry has evolved tremendously with the invention and adoption of modern equipments or tools and wearable devices to perform surgeries, to detect and diagnose various chronic disorders. Though, the usage of modern equipments has reduced the burden of healthcare providers but also improved the precision, accuracy and efficiency of treatment (Bhuiyan et al., 2021). During the COVID-19 pandemic the usage of Internet of things (IoT) enabled devices has accelerated in healthcare sector to provide medical aid to the patients in several ways such as, to fetch the real-time health parameters of the patients, to monitor the stability of patients remotely, to establish a secure communication channel between the patients and healthcare providers, to track the patients and drugs from various hospitals and cities etc. However, the usage of IoT tools has transformed traditional healthcare system by changing the approach of providing efficient services to the patients with various disorders (Javaid & Khan, 2021).

IoT has become one of the most essential parts of modern life; with latest technologies IoT has revolutionized the traditional operations of various organizations and industries by adopting smart working environment with the aid of sensor embedded machineries and devices. IoT connects geographically distributed, multiple physical computing devices capable of sensing, transmitting real-time data through internet (Madakam et al., 2015). However, the IoT ecosystem may include multiple physical devices with minimal computing and storing capacity aiming to perform a specific task. According to the current statistics by 2025, there will be 152,200 IoT devices connecting to the internet per minute and 83% of the organizations have improved their efficiency by introducing IoT technology in their business logic (Kapoor, 2021). These statistics shows that the present generations have endorsed IoT enabled devices in every aspects of life. IoT is a multidisciplinary hence it fits in almost all domains resulting in smart ecosystem such as smart industry (Aleksic, 2019), smart home (Alaa et al., 2017), smart agriculture (Prathibha et al., 2017), and smart healthcare (Baker et al., 2017) by stepping into digital era.

The digitization and IoT (Internet of Things) have revolutionized the healthcare industry by changing everything from the way patients receive care to the way hospitals operate. It plays a key role in diagnostics: from the prognosis of a medical condition or disease, to screening, to diagnosis, to deciding treatment, to monitoring the condition and its progression, to determine long-term treatment modalities and for the prevention of diseases, besides enabling extensive and intensive

* Corrosponding author.
E-mail address: praveenkumarreddy@vit.ac.in (P.K.R. Maddikunta).

https://doi.org/10.1016/j.ijcce.2023.06.002
Received 26 April 2023; Received in revised form 14 June 2023; Accepted 16 June 2023
Available online 25 June 2023

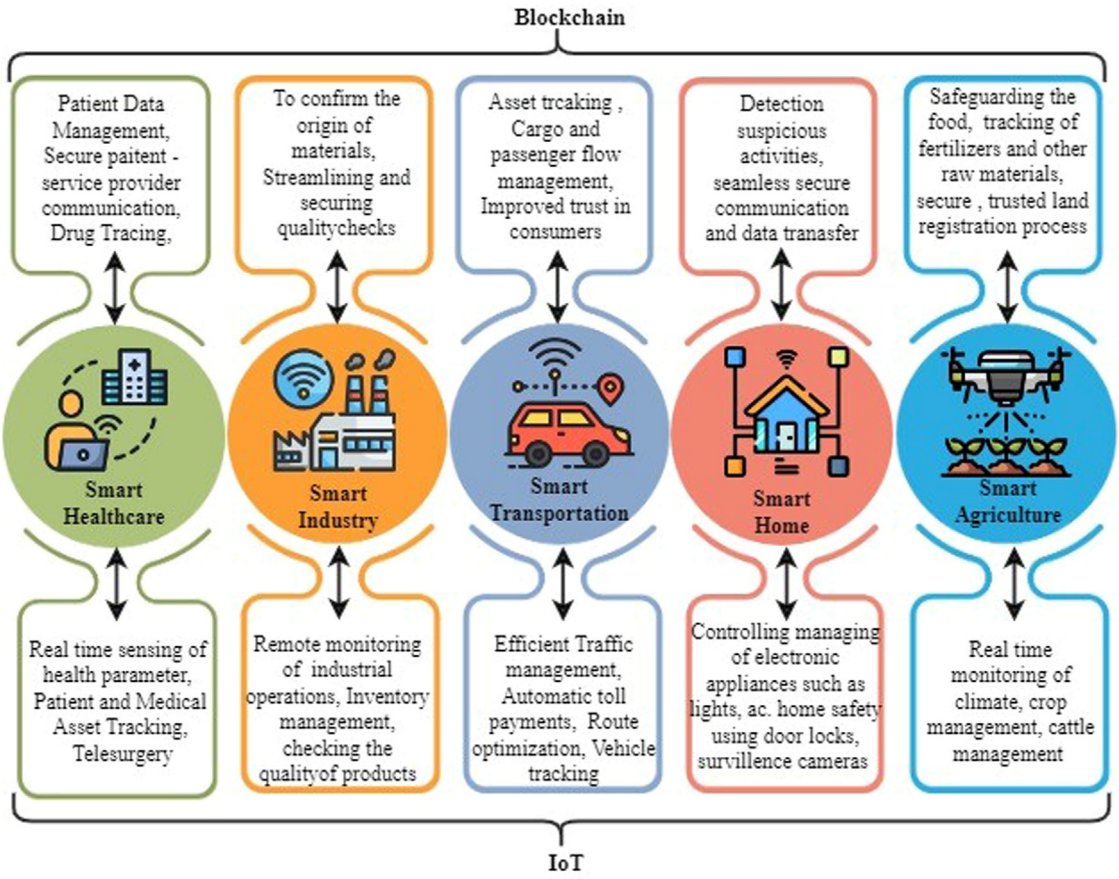


Fig. 1. Usecases of Blockchain and IoT.

research in the healthcare arena (Dwivedi et al., 2022). Hence the adoption of IoT, helps to develop patient's-centric medical services aimed to fulfill the requirement of patients with the well-versed modern equipments combined with modern technologies. For instance, early detection and prediction of chronic diseases such as Heart diseases (Nancy et al., 2022), various types Cancer (Beg et al., 2022; Ramkumar et al., 2022; Karar et al., 2022), abnormal functioning of body organs (Karunanithy & Velusamy, 2022), behaviours of patients (Tiwari et al., 2021) by applying ML or DL models on the data being generated by the body implanted sensors or IoT based medical equipments. An AI-based IoMT treatment support system for needy/remote location COVID-19 patients (Thandapani et al., 2023), a Dilated and Depth wise separable Convolutional Neural Network (DDCNN) model for COVID-19 detection (Li et al., 2021a) and similarly, a IoT enabled smart healthcare system is used to automatically identify and classify the COVID-19 patients based on the chest X-ray (Ahmed et al., 2022). However, in the traditional IoT architecture the real-time data's will be collected through various sensors or the devices/equipments pertaining to the health status of various patients are stored in a centralized storage or the third party cloud (Dang et al., 2019).

On a broader outset every IoT-based healthcare applications consists sensing phase, processing phase and transmission phase, however during the course of different stages the one should consider the life of the resource constrained sensors for the accurate reading, providing security for sensed data, safety of the network, maintain the privacy of data from different attackers/breaches. As the technology evolves the up-gradation of the existing healthcare applications are very much necessary to deliver the effortless services to the patients (Koutras et al., 2020). Blockchain, a Distributed Ledger technology facilitate the conventional, central-server based healthcare application to transform into distributed application, provided with additional guaranteed security and privacy for the medical data. Decentralizing the healthcare system will transform and streamline the communication among the various stakeholders such as doctors, hospitals, insurance companies (Khatri et al., 2021). The tokenization, smart contract and encryption techniques of blockchain will reduce the pre-authorization process hence the patients will directly receive the necessary information efficiently without any delay. The blockchain-based decentralized healthcare platform allows patients to own their data and also allows patients to share their medical records with any doctors (Goel, 2022).

However both IoT and Blockchain technologies are implemented together, they will offer solutions to a range of issues, notably in the field of health care where real-time data monitoring is crucial. The major concerns of the healthcare sector—interoperability, security, and liability—can be effectively solved by utilizing blockchain technology (Banotra et al., 2021). Fig. 1 represents importance of Blockchain and IoT in developing smart systems. For instance, even though the IoT based remote patient monitoring application are efficient in providing accurate services, enforcing the system with blockchain-based hierarchical data sharing framework (BHDSF) will strengthen the personal health record sharing service interns of security and integrity (Zhang et al., 2022). GarliMediChain – a blockchain-based anonymous system provide anonymity and privacy while sharing covid-19 information (Samuel et al., 2022) among the healthcare providers.

1.1. Motivation

According to the recent survey there will be about 30.9 billion IoT connected devices by 2025. Statistics shows, every second on an average of 127 new IoT devices are connected to the web (ServUsTECH, 2023). Hence the IoT adoption rate is huge in various application domains. The major role of IoT in healthcare sector is to continuously monitor the pa-

Table 1
Comparison of proposed research article with the existing survey articles on Blockchain and IoT integration.

Refs.	Application	Overview on Blockchain and IoT and State-of-art	Enabling Platforms	Use-cases	Challenges and Open issues	Future Directions
(Sadawi et al., 2021)	General	√		√	√	
(Shammar et al., 2021)	General	√			√	√
(Nartey et al., 2021)	General	√			√	√
(Haleem et al., 2021)	Healthcare	√		√		√
(Azbeg et al., 2022a)	Healthcare	√		√	√	
Proposed article	Healthcare	√	√	√	√	√

tients' health parameters using several body implanted sensor, IoT based wearables and modern IoT equipments. But existing IoT systems face several issues such as heterogeneity of IoT systems, poor interoperability, resource-constrained IoT devices, and privacy, security vulnerabilities. However, IoT alone will fail to fulfill the requirements of healthcare sector in an efficient manner; hence the incorporation of Blockhain Technology will complement the existing IoT systems by enhancing the interoperability and improved privacy and security. Blockchain and IoT integration will strengthen the self-decision and trust issues among the communicating IoT devices by enhancing the security thus transforming a traditional, centrally controlled client server model into a distributed decentralized model.

1.2. Contributions

Our study focuses on the issues of existing healthcare applications, and challenges related to BCIoT Healthcare services. We investigated a wide range of blockchain and IoT applications by focusing on the objectives, data, platform, and use cases of healthcare sector. We have highlighted the various issues and possible solutions for BCIoT based healthcare applications. Additionally, considering the advantages of present emerging technologies we have also suggested strategies to overcome the shortcomings of conventional healthcare systems. Table 1 depicts the comparison of our study with the existing survey.

Our unique contributions of this research can be summarized as follows,

- We provide a detailed state of art on BCIoT integration for Healthcare applications with highlighting the basic architecture, core components, advantages and challenges of IoT and Blockchain Technology and also a comprehensive discussion on the technical aspects and motivations for the integration of BCIoT.
- We present a detailed discussion on several existing enabling platforms for BCIoT integration.
- We highlight the incorporation of Blockchain and IoT technology to resolve the issues of Health applications such as Remote patient monitoring, electronic heath record management, Health asset tracing, Covid-19 infected patient contact tracking.
- We have explored impact of incorporating BCIoT integration on Healthcare application and identified the challenges. Some future research directions are also suggested to extend the scope of BCIoT in future Healthcare services and applications.

1.3. Paper organization

The rest of this paper is designed as follows: Section 2 introduces an overview of IoT technology, Blockchain technology and further detailed discussions on existing works of BCIoT in Healthcare. Section 3 discusses the major uses cases of integrating Blockchain with IoT in Healthcare. Section 4 discusses the existing platforms for implementing BCIoT architecture. Section 5 discusses some challenges and open problems that obstacle building Blockchain-IoT networks in Healthcare. Section 6 highlights the future research directions in BCIoT for Healthcare domain. Finally, Section 7 summarizes the general conclusion.

2. Background

In this section we discuss about the three layered IoT architecture, challenges of the centralized IoT systems. Later we will give a brief introduction to Blockchain then we will discuss the various evolution stages along with the types of Blockchain, fundamental components of Blockchain and various characteristics of Blokchain. Further we will highlight the possible integration options for Blockchain and IoT along with the various existing works on Blockchain and IoT for healthcare application.

2.1. Overview of IoT technology

Today the Internet has become ubiquitous, has touched almost every corner of the globe, and is affecting human life in unimaginable ways. Internet is the stepping stone for an era of even more pervasive connectivity where a very wide variety of appliances will be connected to the web. The extended version of the internet has lead to the evolution of Internet of Things (IoT). The word IoT was first coined by Prof. Kevin Ashton in 1999 while describing a system of physical world devices/ objects considered as "Things" connecting to the Internet. In general, IoT can be defined as "the interconnection of machine and devices through the internet, enabling the creation of data that can yield analytical insights and support new operations" (Vermesan & Friess, 2022). Every object in IoT ecosystem can be identified as nodes that are interconnected to each other allowing them to send and receive gathered information. The IoT systems are designed to perform a specific task. However, in real-time, objects in the system are enabled with sensing elements, micro-controllers, communication protocols, and information storage and retrieval facilities for establishing faster, active and seamless communications in the IoT system (Lombardi et al., 2021). IoT systems are encompassed with four main component collections - (i) Sensors and actuators, (ii) Gateways, (iii) Network infrastructure such as Routers, Aggregators, and Repeaters (iv) Data Storage Units (Chander & Kumaravelan, 2020).

2.1.1. IoT architecture

IoT technology is a combination of enormous geographically distributed IoT devices, which will interact with smart computing components to perform a specific task. As per the requirement of the application the users will design IoT architecture with the basic functionalities to carry-out the task. The general three layered IoT architecture consists of Perception Layer, Network Layer and Application (Kakkar et al., 2021) represented in the Fig. 2.

- Perception Layer: The perception layer is the lowest layer, where physical devices like sensors and actuators actually perceive and gather the real-time data from the environment that is needed for the application for further computations and also identifies the other devices. Perception layer is sometimes referred to as the physical layer or the device layer, which includes controllers, sensors, actuators, RFID tags.
- Network Layer: Is the communication layer to transfer the collected information from perception layer for further processing. However,

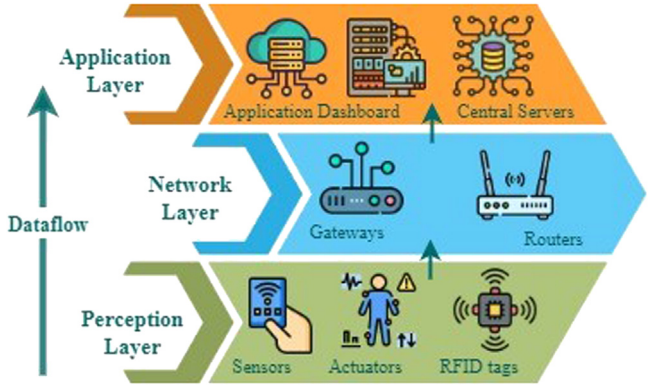


Fig. 2. Three layered IoT architecture.

network layer acts as a mediator by connecting physical devices to other smart objects, servers and other network components.
- Application Layer: Is the topmost layer where the users will interact and fetch data. The processed information's are analyzed and results of the particular task are rendered through the applications.

The adopted IoT architectures are centralized in nature, where the data collected from the perception layers through the various sensors are transferred to centralized remote storage system or cloud storage for further processing and analysis. The centralized architecture allows the central management of the entire IoT network, processing of the operations through the central server (Sethi & Sarangi, 2017). However the nodes participating in the networks acts like a terminal connected to the server and the collected data from the sensors are stored in a single location.

2.1.2. Challenges

- Security: A combination of heterogeneous IoT devices, spread across the network to perform a desired task, requires a major security concerns at different stages of processing to ensure the safety of data from attackers. The existing security solutions such as authentication, authorization, communication encryptions does not suit the resource constrained IoT devices. Edge devices at the physical layer are more prone to attacks such as Distributed Denial of Service (DDoS) resulting in compromising the services by the group of malicious IoT (Malhotra et al., 2021).

Privacy: Privacy in IoT is protecting the information of the individuals from exposure without explicit consent regardless of any situation. In an IoT network the collected data from the environment will be transferred to server or events to perform a specific task, however, during the process the privacy must be guaranteed in device/sensors, storage, communication, and processing to avoid unauthorised access, to maintain the data confidentiality. Since the IoT devices are usually resource-constrained with limited capabilities and have weak access points to complex smart infrastructures which lead to leakage of sensitive data (Kagita et al., 2022). Similarly, the complex heterogeneous architecture of IoT network not only complicates the development of protocols as well as the system operations. Hence the proper measures/policies need to be considered for the user anonymity, user identification, user tracking, data summarization and data access (Tawalbeh et al., 2020).

- Interoperability: It is the ability of the system components to interact with each other irrespective of their specifications and compositions without affecting the normal functioning of the system. However, the IoT system contains heterogeneous components with diversities in specifications, functionalities and operations, hence achieving interoperability across the system using a common IoT service layer is still a challenging task. Since the IoT technologies are being adopted across various domains, as the number connected devices increases, network expands, requirements changes maintaining interoperability of the system becomes the highest priority (Samizadeh Nikoui et al., 2021).
- Scalability: Scalability is the capability of a system to handle the extra workload requirements while adding additional resources. As per the requirement of a user, the adopted IoT systems must be in a position to process the requests adhering to the developers attributes and without compromising the overall performance of the system. Irrespective of the type of the scalability operation i.e. vertical and horizontal, the IoT ecosystem is complex in nature, massive scaling operations will be a challenging task because adding sensors to the existing ecosystem requires adaptive scalable routing scheme for a huge collection of sensors. The IoT cloud integration with dynamic management and resource provisioning will resolve the additional overhead caused due to scalability, also the adoption of MQTT and CoAP protocols support network scalability by providing guaranteed support for resource-constrained and unconstrained devices (Farhan et al., 2018).
- Heterogeneity: IoT ecosystem is a combination of geographically distributed heterogeneous physical IoT devices, hetero- geneous network protocols and diversified structured, unstructured, semi-structured IoT data types. However, the main concern in every IoT base system is to design a common procedure or platform to abstract the heterogeneity of components by maintaining their actual functionalities to perform a desired task without any hindrance. While designing IoT based applications service providers need to concern about the adaptability of the system for the diverse network protocols, communication procedures and evolving versions of hardware and software for various IoT devices (Ali et al., 2018).

2.2. Overview of Blockchain

Over the past decade, the concept of Blockchain has emerged as one of the most promising technologies in academia and industry. The concept of Blockchain was first introduced by Satoshi Nakamoto in a white paper in 2008, as an underlying technology for Crypto-currency (Nakamoto, 2008). Blockchain can be defined as a decentralized, distributed, immutable ledger used to securely record transactions across many computers in a peer-to-peer network without the need for third parties. Basically, the Blockchain works on the principles of Distributed Ledge Technology (DLT); hence, Blockchain is a form of Distributed ledger. Unlike the centrally controlled Client Server Model, a DLT works in a distributed shared environment, where a ledger or database is shared among the several computers, nodes or peers future allowing users to continuously access, validate and update the transaction related data (Frankenfield, 2023). When a ledger database is shared among the nodes, each individual nodes will replicate and maintains a copy the database for future modifications. Since the entire process in DLT works in a distributed ecosystem there will not be any central authority (Farahani et al., 2021). But, the Blockchain maintains a unique structure for storing the transactional data *via* Blocks. Individual blocks in a Blokchain are cryptographically connected together to form a secure and unbreakable chain. Each block in a chain consists off block header with timestamp indicating the published time of the block time, nonce which is a randomly chosen number that miners would regularly alter to get a certain hash value to resolve a mathematical puzzle, a Merkle tree that fundamentally decreases the exertion required to check transactions inside a block and block body consists of confirmed and validated transactions. However, the first block of the Blockchain is called as the "genesis block", which doesn't have any parent (Ali et al., 2021) and the basic structure of block chain is represented in the Fig. 3.

2.2.1. Generations of Blockchain

Blockchain is a real game changer for most of the real-world problems by introducing new possibilities, applications in several domains.

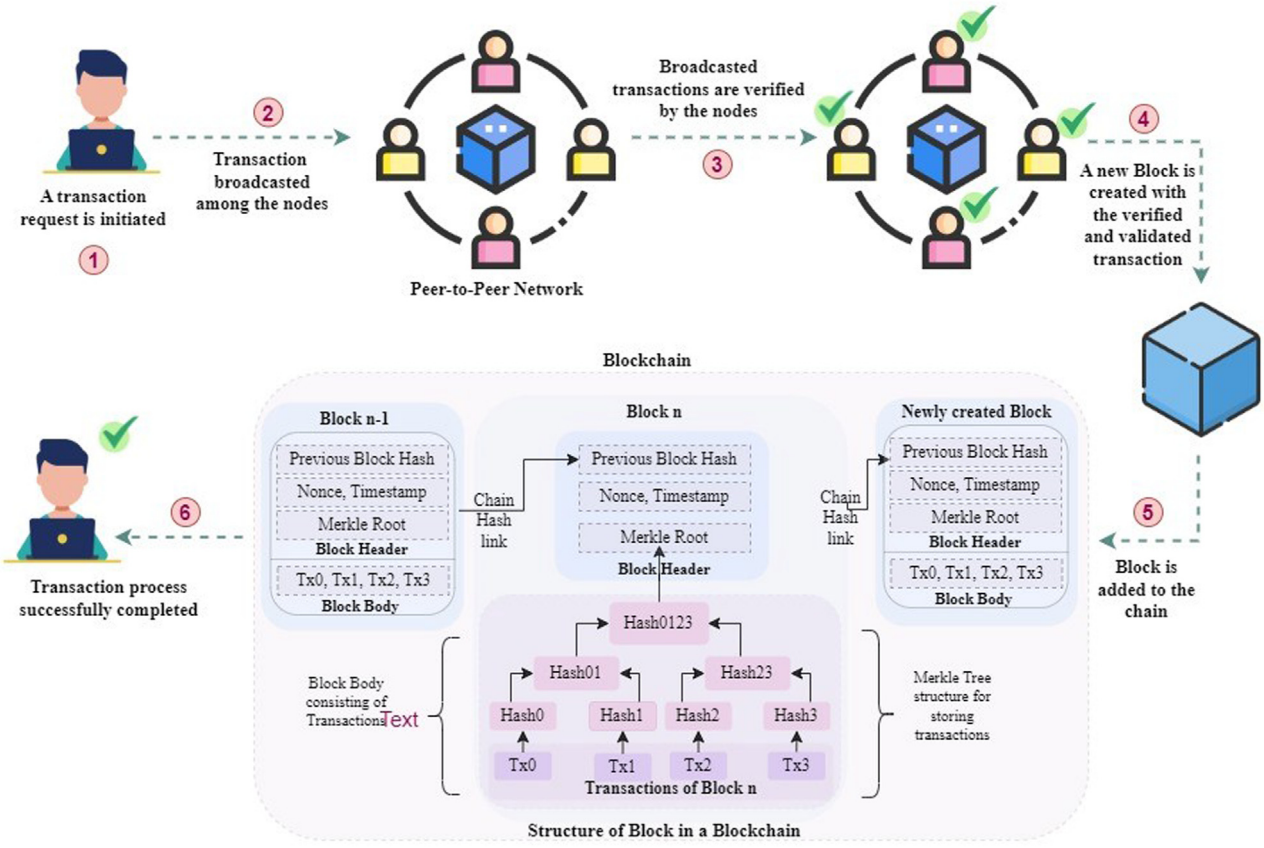


Fig. 3. Transaction processing in Blockchain and Blockchain structure.

Ever since the invention of blockchain, many researchers and organizations have contributed to the development of three different stages Blockchain 1.0, 2.0,3.0,and 4.0 (Farahani et al., 2021).

- Blockchain 1.0: Is mainly applied to digital currency, where Bitcoin is the most dominating one, and the application is limited to storing and transfer of value.
- Blockchain 2.0: Supports the creation of advanced smart contracts, extending the doors for new application areas, enabling different industries to collaborate through applications, enabling automation of resource allocation by resolving the mutual trust and identity among the participants.
- Blockchain 3.0: Has emerged as application-centric by allowing blockchain to confirm the property rights of the information values on the Internet. Hence blockchain can be used to track and control assets while trading. Apart from that, blockchain has also extended its scope in various domains, such as health, identity certification, logistics, and voting.
- Blockchain 4.0: Is the emerging blockchain version aim to deliver business usable platform by converting technology to mainstream. Blockchain 4.0 allows the incorporation of AI and the integration of various platforms under the single hood to accomplish the requirements of industry.

2.2.2. Types of Blockchain

The Blockchain can be broadly categorised into three different classes as Public, Private and Consortium (Islam et al., 2021).

1. Public Blockchain: Public Blockchains are also known as Permissionless Blockchain, where any individual can participate in transaction and mining process by joining the network without the seeking for any prior permission. In the public Blockchain the individual's identities are unknown; however, individuals joining the network as miners can access the block details from the network and initiate the mining activity, also allowed to create blocks in the network resulting in more vulnerable to Sybil attacks, selfish mining, and 51% attack (Sanka et al., 2021).
2. Private Blockchain: Private Blockchains are also referred as Permissioned blockchain, where only trusted entities are allowed to join the network with prior permission from the owner. Only the authorized users are allowed to access the block details, transaction validation and can participate in mining process. The private blockchain is a closed centralised ecosystem where activities are managed by single owner; hence it is more scalable, less prone to Sybil attacks, selfish mining, and 51% attack (Sanka et al., 2021).
3. Consortium Blockchain: Consortium Blockchain is a combination of both private and public Blockchain. Basically the consortium Blokchain is managed by owners for sharing information with little or no trust. However only a selected set of nodes can participate in mining and transaction process, can create new block and remaining nodes can only send and view transactions, can access block details, can verify the blocks. Consortium Blockchain has less privacy and security and no 51% attack (Sanka et al., 2021).

2.2.3. Transaction processing in Blockchain / working of Blockchain

A blockchain transaction has to undergo several steps before it becomes a part of the blockchain, a critical aspect of the technology being the way it authorizes and confirms transactions. The following steps are carried while processing a transaction in the blockchain and it is also represented in Fig. 3.

1) A new transaction request is initiated by the user.
2) Requested transaction is broadcasted among the nodes in the peer to peer network for verification.

Table 2
Comparison of the various consensus algorithms.

Consensus Algorithm	PoW	PoS	DPoS	PoC	PBFT	Raft
Blockchain Type	Public Blockchain	Public Blockchain	Public Blockchain	Public Blockchain	Private and consortium Blockchain	Private and consortium Blockchain
Transaction finality	Probabilistic	Probabilistic	–	–	Immediate	Immediate
Miner election process	Solving puzzle	Stake Owned	Stake Owned	Storage capacity	Mathematical operation	Randomized timer
Consensus category	Proof-based	Proof-based	Proof-based	Proof-based	Vote-based	Vote-based
Computational Overhead	High	Medium	Medium	Low	Low	Low
Storage Overhead	High	High	High	High	High	Medium
IoT suitability	Low	Medium	Medium	Low	High	Medium
Advantages	System of nodes are open, Freedom of nodes are of high degree, Steady and secure, High level of decentralization	Less power consumption, High level of decentralization, System of nodes are open	Less power consumption, High performance	Flexibility in using any hard drive, Energy efficient	High performance, Definiteness, Highly secure	Cost saving
Disadvantages	Minimal scalability, Degraded performance, Wastage of Hardware resource	Tough execution process, Safety violation	Less power consumption, High performance	Possibility of malware attack, Possibility of a centralized storage	Fragile amount of decentralization, Blocked node system, Short fault acceptance	Low adoption rate

3) Peer confirms the validity of the broadcasted transaction after getting the approval from all the peers in the network 4.
4) A new block is created with confirmed legitimate transactions.
5) A newly created block is added to the blockchain network.
6) The requested transaction is finally stored in the blockchain network, which confirms the completion of transaction process.

2.2.4. *Major components of Blockchain*

- Node: Any participating user on the blockchain network can be treated as node.
- Transaction: Is the fundamental building block of the blockchain system, generated by the node and later it will be added to Block after the validation process.
- Block: A data structure, which stores a set of valid transactions. The miners are responsible for creating a block after the verification and validation of transactions.
- Chain: Is a cryptographic hash link between the Blocks in a Blockchain. Chain maintains the sequence of blocks in a specific order.
- Miners: A type of node which participate in verification and validation process of the transaction.
- Cryptography: Cryptography prevents the unauthorised access of the private data by ensuring the security, reliability and privacy of transaction in a Blockchain. The cryptographic approach such as Hashing is used to link the blocks and Asymmetric cryptography is used for identifying the contributors and proof of their ownership in Blockchain network (Rahman et al., 2022).
- Hashing: Cryptographic hash functions are used to generate a numeric value of fixed length known as Hash Value, which represents data. Hash functions are one-way function, i.e. we cannot retrieve the data using hash value and every small change in the data will modify the hash value. SHA256 hash function is used to represent the state of the Blockchain.
- Digital Signature: Implements an Asymmetric cryptography using private and public key to authenticate the users before providing access to the private data. Blockchain consists of Signing and Verification phase, where, every transaction is signed using private key and is broadcasted over the network and later the transactions are accessed *via* public key by the network users.
- Merkle Tree: Is also referred as the Hash Tree. Merkle trees are mathematical data structures that serve as an overview of all transactions in a block of data by combining hashes of several blocks of data. It is used for efficient and secure verification of huge data by confirming the accuracy and integrity of the data.
- Smart Contract: Computer programs that automatically performs specified task when a particular condition meets. Smart contract consists of agreement policies, to enable the trust less and permission less transactions between the users without the help of intermediary.
- Consensus Algorithm: Blockchain is a decentralized peer to peer network, where the block generation will happen based on the consent of all the peers. It is challenging to achieve the consensus in a trust-less distributed ecosystem where all the peers connected to the network will participate in block validation process, however trustfulness in validation is attained using consensus algorithms an agreement to gain the mutual trust among the peers without using any trusted third party authority (Lashkari & Musilek, 2021). Based on the working principles, consensus algorithms are divided into two categories such as Proof-based consensus algorithms and Vote-based consensus algorithms (Saxena et al., 2021). The most widely used and popular consensus algorithms are summarized below also represented in Table 2.
- Proof-of-work (PoW) : PoW is a validation method that utilizes the computational power to check blocks and stop forgery. The reward for that block goes to the miners who figure out the puzzle. However, soon after the consensus process the newly generated block is added to the chain. Due to the concurrent production of blocks, a blockchain may occasionally fork into multiple branches. This problem can be addressed by assuming that the longest chain of valid blocks will exist. This offers a method of distributed consensus without trust (Kaur et al., 2021).
- Proof of Stake (PoS): PoS, is an alternative to PoW consensus and it is proposed to reduce enormous amount of resource usage utilization of PoW consensus algorithm. PoS introduce a “forger” instead of miner. The “forger” will be selected based on the value stakes that the node has after each consensus process (Kaur et al., 2021). More the number of stakes resulting higher the chances of being selected as a forge for creating a new block hence the number of nodes participating in the mining process are reduced. Although the PoS consume less computational power, but it results in “nothing-at-stake” problem (Gu et al., 2021).
- Delegated Proof of Stake (DPoS): The DPoS is an extension of PoS consensus, where representative democratic principles are implemented. DPoS introduces Witnesses and Delegates nodes from set

of nodes *via* voting process. Witness nodes are responsible for creating a node and Delegates are responsible for maintaining, generating, verifying and adjusting of block size in the network. However, the number of nodes participating in mining process will result in increased transaction execution (Majumder, 2022).

- Proof of Capacity (PoC): It is developed as an alternative solution for PoW and PoS, where the available storage capacity is used for mining operation and transaction validation hence it is also known as proof of Space. Unlike PoW and PoS which uses computing hardware and stakes for mining but PoC allows miners to exchange their work, time factor with storage space aiming to preserve computing power required to find hashes. Hence PoC is energy efficient and consumes less time to process the transactions (Azbeg et al., 2021).
- Practical Byzantine Fault Tolerance (PBFT): Is a voting-based consensus algorithm, works based on the principles of Byzantine Fault Tolerance. During the consensus mechanism a primary node will be selected from a set of Nodes as a leader node, responsible for leading the consensus mechanism and creating the block after verification. There will be three phases in every block validation stage called as views: pre-prepare, prepare and commit. As soon as the primary receives the transaction request from the client, Primary initiates the prepare phase by sending a new block proposal with the transaction request to all the nodes. During the Prepare phase the nodes will accept the block request and sends an acknowledgement back to all the nodes as an approval for the creation of new block. After receiving 2f+1 prepare message from the different nodes, commit phase will resume where the verification and validation of proposed block requests done. At the end of commit phase nodes will send a commit message to other nodes confirming the request for block creation. The new block will be added to the chain by the primary node only after receiving 2f+1 commit messages from various nodes (Meshcheryakov et al., 2021) (Table 2).
- Raft: Raft is a voting-based consensus algorithm which maintains a distributed, consistent, append only log known as replicated log which is shared among all the nodes in the network. Raft consensus mechanism includes two stages: leader election and log replication and every node in the network exhibit any of the three roles such as follower, leader and candidate. The consensus process starts with a leader election and leader is responsible for ordering the transaction and managing of replicated log. Once the leader is selected the log replication stage will be initiated, where the leader receive log from clients and creates a transaction log in the server (Xiong et al., 2022).

2.2.5. Characteristics/Features of Blockchain

The origin of Blockchain has shown a lot of advantages in various domains by enabling new opportunities to solve problems in a trustless environment. Blockchain technology exhibits several unique characteristics such as,

- Decentralization: In a centralized system, single central authority or a third party will take the responsibility of maintaining and managing of data, transaction or data verification, authorizing the peer nodes hence the system complexity will increase resulting in reduced performance and single point of failure. In contrary to the central architecture Blockchain is not managed by any single authority, every nodes participating in the network will verify and validate the transactions, and also block will be generated based on the consent of all the peer nodes. However, Blockchain a distributed ledger technology is less prone to attacks and other malicious activities with improved performance of the overall system in comparison with traditional central architecture (Atlam & Wills, 2019).
- Immutability: The every block in a Blockchain are linked to each other using a hash of the previous block, however if the attacker or any peer tries to tamper the content of any block then the corresponding block hash, and transaction details in the Merkle tree needs to be modified and updated in every successive blocks of the chain; however, practically it is infeasible in case of large network. Any minor changes to the data in the Blockchain can be easily identified hence through Immutability property of Blockchain data integrity can be achieved among the nodes (Atlam & Wills, 2019).
- Improved Security: The decentralized architecture of Blockchain distributes the data across the network rather than storing the entire data in a single central location which reduce the risk of data being tampered. Also the sensitive informations that are stored in the individual blocks are in cryptographically encrypted and blocks are interconnected through the hash values. Because of these features the visibility of the data being protected from the attackers and also can improve the security across the chain (Atlam & Wills, 2019).
- Transparency: Blokchain is a shared distributed ledger, where the same copy of the ledger is shared among the peers in the network. Every node connected to the Blockchain network will have a copy of the immutable, accurate, consistent documentations about the activities happening in the network and also have the access to the verified transactions. Every node will maintain the details of the other node participating in the mining activity. Hence Blockchain does not require any third party authority to maintain the trust among the nodes (Atlam & Wills, 2019).
- Traceability: Blockchain maintains a ledger with every details of the transaction such as origin, validation, verification, execution status along with the timestamp, hence it will be very easy for the individual to trace or track the transaction. However, all the committed transaction details that are stored in the ledger are permanent and nobody can change it. The historical data related to a particular medicine stored in the blockchain can be used to track its availability in Medical domain (Yaqoob et al., 2021).

2.3. BCIoT integration

IoT has experienced exponential growth over the past several years, opening up a wide range of options for access to and sharing of information. Even though the IoT technology has resolved the issues of traditional systems by modifying the business logic and operations in several ways but the issues caused during the process of managing the information requires proper attention. Hence, the integration of Blockchain and IoT will not only provides the solutions for the issues of IoT based systems but, it will be a major step towards developing a verifiable, safe, and effective means of storing data processed by ”smart” devices. Fig. 4 represents the various communication reference models for the Blockchain IoT integration. During the integration process the interactions of the IoT devices and the blockchain can happen through either of the following ways,

- Device to Device Model: In this model the IoT nodes will perform the specific communication or task using routing and node discovery techniques, outside the premises of the Blockchain network. Only a metadata of the transactions are stored in the Blockchain (Torky & Hassanein, 2020). Hence, the blockchain is used as a store component for IoT devices. This type of model can be used in an application where low latency and high performance are of major concern (Saxena et al., 2021).
- Device to Blockchain Model: In this model all the IoT devices performs the specific task or the communication using blockchain network. Each and every operations detail is recorded in the blockchain. Hence the blockhain can be used as a data storage component and also to monitor and manage transactions. Since the transactions are stored in the blockchain, model provides the transparency and traceability of interactions. This type of model can be used in a system involving communications between several IoT devices of distinct domains but model induces bandwidth overhead due to the huge amount of transactions and IoT data being stored in the blockchain (Torky & Hassanein, 2020).

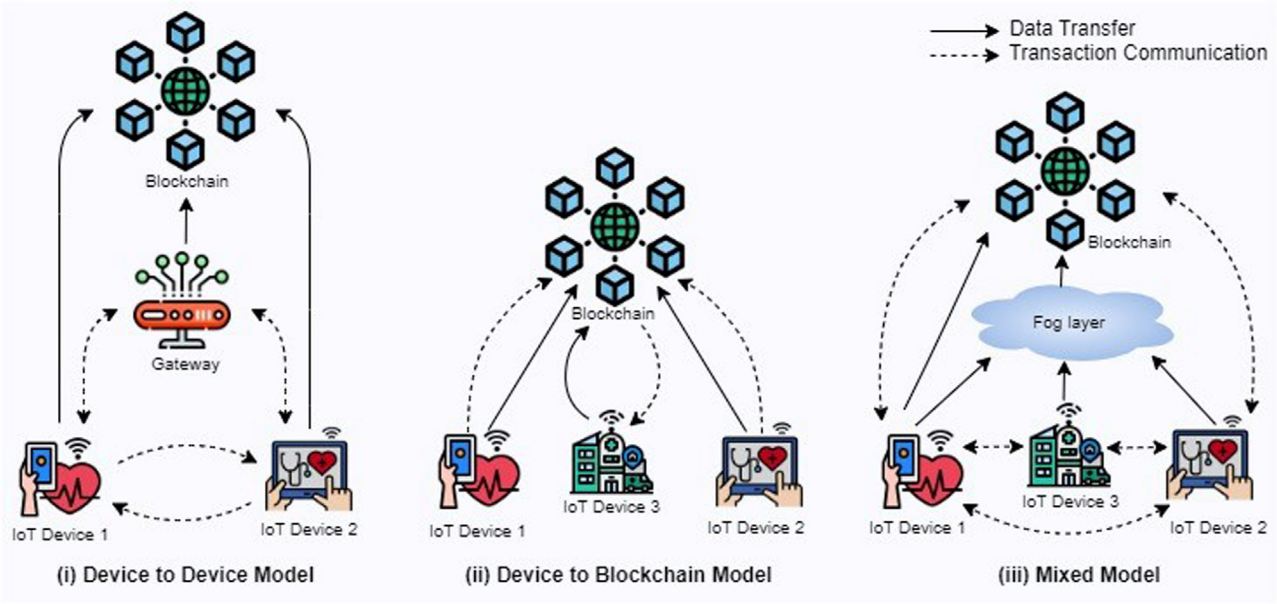


Fig. 4. Blockchain and IoT integration reference architecture.

- Mixed Model: Is an improvised version of the IoT to blockchain Model, where the IoT users are given the choice to select the blockchain network for certain event interactions and remaining events will happen directly through IoT devices. But the segregation of interactions for blockchain network and IoT devices will happen only during the runtime hence to optimize the operations and to achieve the best integration of IoT and Blockchain to utilize their features without compromising on issues, hence the model employ Cloud or Fog Computing (Torky & Hassanein, 2020).

2.4. State of art

Healthcare sector is one among the most evolving domains interns of providing accurate services to the patients with the help of IoT technologies. The promising features of IoT devices or equipments have not only reduced the possible human errors but also strengthened the traditional medical services in various aspects, hence, resulting in increased adoption to perform activities such as remote patient monitoring, electronic medical record management, track patients during pandemics, track drugs availability, trace the drugs during the transport, accurate disease predictions and prescription suggestion. Early detection and prediction of disease using IoT devices or equipment's and AI technologies with Machine learning and Deep learning models have increased the efficiency of medical services. Gao (2021) has proposed a gray level co-occurrence matrix with extreme learning machine for early detection of Alzheimer – a neurodegenerative disease in patients using medical images. Ahmed et al. (2021) has proposed a ML based technique to identify the patients suffering from various types of diabetes using their clinical data. Li et al. (2021b) has proposed multi-modal medical image fusion technique to improve the medical diagnosis. However, during the COVID-19 pandemic as a precautionary measure, individuals are compelled to wear mask and maintain social distancing in public places to break the chain of spread or to avoid the transmission of the disease. Hence the authors Prasad et al. (2022) has proposed COVID Vision with CNN model to detect the face mask and track the social distancing using real-time data. The proposed model also compared with several existing algorithms. Similarly to support the Hearing impaired people, using IoT devices and modern technologies, Kumar et al. (2022) has proposed a visual speech recognition system with an efficient lip reading mechanism using deep learning models. Along with monitoring the health parameters, recognizing the Human activities in remote patient monitoring is a challenging task. However, the authors Muralidharan et al. (2021) has proposed a feed forward neural network and 1D CNN model to classify the human activities having accelerometer and gyroscope values recorded through smartphone under the several labels such as Walking, Walking Upstairs, Walking Downstairs, Sitting, Standing, Laying. The authors also analyzed the proposed model with existing machine learning algorithms for the better understanding and further enhancement. Strengthening the activities of resource-constrained IoT devices without draining the sensors in a large network is another major challenge, hence a Scheduling Algorithm based on Learning Automaton will improve the stability IoT devices during the data transmission by ensuring minimal energy consumption (Sangaiah et al., 2023) and a neural computing-based access control protocol will improve the security and privacy of the AI driven intelligent systems (Mahmood et al., 2023).

Although aforementioned approaches improve the accuracy of medical diagnosis in various aspects but the security and privacy of the medical data is still under risk. Since, almost every medical services deal with critical informations related to various patients and the drugs, thus it expects the incorporation of strong security, privacy and access control methods during the various stages of providing service such as data collection, transmission, storage and manipulation. The recent evolutions in the field of Blockchain technology has shown the promising outcomes interns of providing security to the sensitive information as well as the IoT devices. The authors, Srivastava et al. (2019) has proposed blockchain based approach for securing the IoT based remote patient monitoring system using ring signature cryptographic technique. RPM is a powerful and real-time patient monitoring approach with the aid of body sensors at any time, irrespective of their location (Hathaliya et al., 2019). Srivastava et al. (2021) has proposed a detailed study on the ethical issues while incorporating blockchain technology in health care applications, however the authors have identified the issues that are need to be resolved by various parameters associated with blockchain based healthcare applications, also highlighted the ethical and network communication dilemmas and proposed several road map techniques for the efficient adoption of ethical blockchain in healthcare. Since RPM is a continues process the size of data being generated will be huge and the sensors are equipped with limited resources hence to carry-out the monitoring process without any hindrance, Uddin et al. (2018) has proposed tier-based architecture with blockchain enabled patient centric agent (PCA) for the continues patient monitoring. End to end security is achieved using lightweight authentication protocols with dy-

namic sessional symmetric keys. The proposed model outperforms the existing architectures. Along with the security of medical data maintaining the privacy of patients is a challenging task in RPM, hence authors Zaabar et al. (2021a) has designed a Blockhain based access control mechanism using hyperledger fabric. The experimental results have shown better performance compared to the public ethereum blockchain frameworks, However, the model can be strengthened by considering the various privacy and security issues for analysis and interoperability of the system can be verified by considering other IoT frameworks. In a traditional IoT ecosystem of RPM, protecting the sensed data will be a challenging task, during the process of sharing data from physical layer to the higher layer for further analytics the data may be tampered by the attackers, intrusion of malicious users may lead to loss of entire network however to resolve data security and identity security issues the authors Xie et al. (2023) proposed TEE-and-Blockchain-supported IoT data sharing architecture(TEBDS) a combination of on chain and off-chain method. Considering the possible issues while exchanging huge data among multiple e-health entities in automated patient monitoring systems the authors Abdellatif et al. (2021) has developed a Medical-Edge-Blockchain (MEdge-Chain) by integrating blockchain and edge computing aimed to process enormous medical data. The queuing based priority assignment procedure will process the transactions based in the priority in the blockchain while collecting data from multiple entities at the same time efficient patient management procedure at the edge will improve the response time.

The conventional EMR system uses central cloud server to store and manage the health records, where each and every operations will happen through the third party service provider. To avoid the single point of failure of the central server, data tampering, and the involvement of third party agents, Akhter Md Hasib et al. (2022) has designed a smart contract based blockchain framework for monitoring the electronic medical records. Maintaining the integrity of the EHR data without losing the privacy of patients during the outsourcing process is another concern in traditional models. Huang et al. (2021) has proposed Blockchain based eHealth system (BCES) to audit the every manipulations of EHR. Their model implements attribute based proxy re-encryption for access control. Fatokun et al. (2021) has proposed a cross platform compliant, patient-centric EHR system aimed to avoid the involvement of third party organizations while controlling and managing of EHR. The medical records from various providers are collected and stored using a unique format to ensure security and privacy. Similarly the authors Dewangan and Chandrakar (2022) has proposed a Blockchain-based Patient centric data collection system, where the patients will use personal digital assistant (PDA) to transfer their medical data to cloud server. The authors have also introduced a novel miner selection procedure to avoid the bias in the blockchain. The proposed model is tested by simulating various attacks between IoMT devices and Cloud server. The system results in minimal communication overhead hence the overall performance of the system is less compared to the existing models. Nie et al. (2022) has introduced a secure EHR sharing system among multiple users using blockchain and IPFS with time bound and verifiable search protocol. The smart contracts are used to implement secure search procedure on Ethereum network. Model outperforms the existing models with minimal computation overhead and computational cost.

Apart from the conventional applications, integration of Blockchain and IoT has led to the development of tremendous applications during the COVID-19 pandemic. The many healthcare providers along with the team of researchers have developed several frameworks to provide efficient medical services such as Disease Control, Traceability, and Tracking of healthcare instruments (Sharma et al., 2020). Another most interesting implementation of blockchain and IoT is to trace the patients contact during pandemic. To reduce the spread of the virus through physical contact, the authors Zhang et al. (2021) has proposed 5G-integrated and blockchain-based medical application with privacy-preserving contact tracing scheme. A decentralized contact tracing scheme will identify the contact of an individual with the diagnosed patient without revealing their actual identity and location. Table 3 depicts the summary of existing Blockchain and IoT based Healthcare applications.

3. Blockchain platforms for IoT integration

In this section we discuss the different features of the existing platforms such as Hyperledger fabric, Ethereum, Quorum and Multichain, that supports the integration Blockchain and IoT for various applications of Healthcare sector. The comparision of existing blockchain platforms are reperesented in Table 4.

3.1. Hyperledger fabric

Hyperledger is an open-source Blockchain platform aimed to advance the cross-industry Blockchain technologies through collaborative approach, initiated in 2015 by Linux foundation (Foundation, 2023). Hyperledger is an umbrella of various projects and Fabric is one among those projects. Hyperledger Fabric is a modular framework; hence it supports various pluggable services and components such as consensus, membership which helps to create enterprise solutions in various domains such as Healthcare, smart city, agriculture, industry providing privacy of transactions, scalability, flexibility, improved performance, verifying the identities etc. Hyperledger Fabric supports the deployment of private and consortium Blockchain. Fabric adopts unique Execute-order-validate architecture for parallel transaction processing, by replacing the traditional order-execute architecture. Unlike other Ledger technologies, Fabric supports smart contract called Chaincode can be written in various languages such as Go, Nodejs, and Java; used to manage the business logics among all the nodes in the network, allows to impose transaction and network access policies among the nodes. For an instance in Healthcare applications the patients can specify the access permission his/her medical reports hence patients will have the full control over their respective records (Abutaleb et al., 2023). In Fabric network nodes are assigned with different roles such as Endorser Node, Anchor Node, Orderer Node. Endorser node is responsible for transaction validation and execution of chaincode, anchor nodes will broadcast the updates to other nodes in the network, orderer node will create and broadcast the new block among the peers. Fabric supports PBFT consensus mechanism; however every transaction is validated and ordered using consensus mechanism by considering mutual concerns of the nodes contributing for the data integrity among the shared ledger. Hyperledger fabric provides built-in dynamic access control mechanism for IoT devices in Blockchain network (Iftekhar et al., 2021). Due to the significant features of Hyperledger fabric it's been used in various applications of healthcare to maintain the privacy of patients (Stamatellis et al., 2020), to secure electronic medical record (Kothari et al., 2021), to achieve confidentiality, anonymity, traceability while sharing patients' sensitive records with health service providers (Kumar & Chand, 2021).

3.2. Ethereum

Ethereum is a type of Blockchain which exhibits the similar properties of Bitcoin. However, Ethereum a distributed public ledger platform which enables developers to create, run and deploy decentralized applications (Ethereum, 2023). Ethereum Virtual Machine (EVM) enables users interact with Ethereum Blockchain by understanding the smart contracts. Since Ethereum is a permissionless Blockchain, users can create two different types of accounts in EVM such as Externally Owned Accounts (EOA) for users or devices, controlled by the user's private key and Contract Account which is controlled by the smart contract. The geographically distributed nodes can execute the transactions and also participate in the mining activity just by joining the Ethereum Blockchain network. The consensus algorithm which is used to maintain the integrity of ledger across the nodes in the public network is Proof of Work, where the peer nodes will solve a mathematical puzzle using a random

Table 3
Summary of the existing works using Blockchain and IoT in healthcare.

Refs.	Privacy	Data Security	Scalability	Data Integrity	Interoperability	Authentication and Authorization	Energy Consumption	Main Contribution / Remarks
(Srivastava et al., 2019)	MID	HIGH	LOW	LOW	LOW	MID	HIGH	Proposed a prototype for the development of Lightweight cryptographic technique combining Symmetric and Asymmetric schemes.
(Uddin et al., 2018)	LOW	HIGH	LOW	LOW	LOW	LOW	HIGH	Lightweight authentication algorithm and miner selection algorithm (MSA).
(Zaabar et al., 2021a)	HIGH	HIGH	LOW	MID	LOW	LOW	MID	Framework was designed using Hyperledger fabric and it consists of Cloud storage layer, fabric layer and composer layer and RPM layer.
(Xie et al., 2023)	LOW	HIGH	LOW	MID	LOW	LOW	LOW	Proposed model consists of smart devices that users wear, a device service provider(DSP), a consortium blockchain, and a key management center with continues data read/write process
(Abdellatif et al., 2021)	LOW	HIGH	LOW	MID	LOW	LOW	MID	Assigning the priority for the transactions based on the urgency and arrival time, Allocate the transactions to blockchain channel based on the urgency and security levels.
(Akhter Md Hasib et al., 2022)	LOW	MID	LOW	LOW	LOW	LOW	LOW	Blockchain based framework to share X-ray records with physician, Keccak256 cryptographic function in solidity.
(Huang et al., 2021)	HIGH	HIGH	HIGH	LOW	LOW	LOW	LOW	Attributes-based proxy re-encryption technique.
(Fatokun et al., 2021)	HIGH	HIGH	LOW	LOW	MID	LOW	LOW	Patient-centric EHR model.
(Dewangan & Chandrakar, 2022)	LOW	HIGH	LOW	LOW	LOW	HIGH	LOW	Patient centric model to store health data in cloud recorded using IoT devices with novel miner selection algorithm
(Nie et al., 2022)	LOW	HIGH	LOW	HIGH	LOW	LOW	LOW	Searchable encryption and smart contract are implemented with a star chain structure.
(Zhang et al., 2021)	HIGH	MID	LOW	LOW	LOW	MID	LOW	Proposed frame work consisting of Public-key cryptosystem with strong private key decryption and Bloom filters.

Table 4
Comparison of Blockchain platforms for IoT.

Platform	Ethereum	Hyperledger Fabric	Quorum	Multichain
Use case	Generic Blockchain Platform	Modular Blockchain Platform	General Application Platform	General Application Platform
Blockchain type	Permission less	Permissioned	Permissioned	Permissioned
Consensus Algorithm	PoW - PoS	PBFT, Kafka, Raft	Raft, Quorum Chain	Multichain consensus
Smart contract support	Yes	Yes	Yes	Yes
Smart contract Language	Solidity	GO, JAVA, Node.js	JAVA, Kotlin	Javascript
Currency	Ether(ETH)	No built-in currency	No built-in currency	No built-in currency
Hash Algorithm	ethash	SHA256	SHA256	SHA256
Throughput (transactions per second (tps))	upto 20 tps	more than 2000 tps	few 100 s tps	upto 1000 tps
Latency	High	Low	N/A	Low

nonce to satisfy the constraints for creating a new block. Due to PoW consensus algorithm, only 60 transactions can be processed per second, also it consumes enormous amount of energy during the computation of hash value, although Blockchain resolves domain specific issues by providing enormous features, because of drawbacks of PoW consensus the performance of entire Ethereum Blockchain will be affected hence the recent research on the consensus algorithms have developed the alternate options for PoW are proposed such as PoS, DPoS, PoC. With the combination of efficient consensus algorithms and smart contarct the ethereum based blockchain architecture is used in various medical services with the integration of IoT devices such as on- demand health data sharing with the Doctor by the patients by enabling access permissions (Al-Joboury & Al-Hemiary, 2021), smart contract based secure record sharing (Nishi et al., 2022), Blockchain-Enable Smart-Contract Cost-Efficient Scheduling Algorithm Framework (BECSAF) schemes for secure ofloading of patients data (Lakhan et al., 2021).

3.3. Quorum

Quorum is a permissioned blockchain platform developed by JP Morgan to address the issues of financial sector using distributed ledger and smart contract (Quorum, 2023). Quorum has extended some of the features of Ethereum, which ensures the privacy and confidentiality of transactions i.e., apart from the public visibility transactions, Quorum

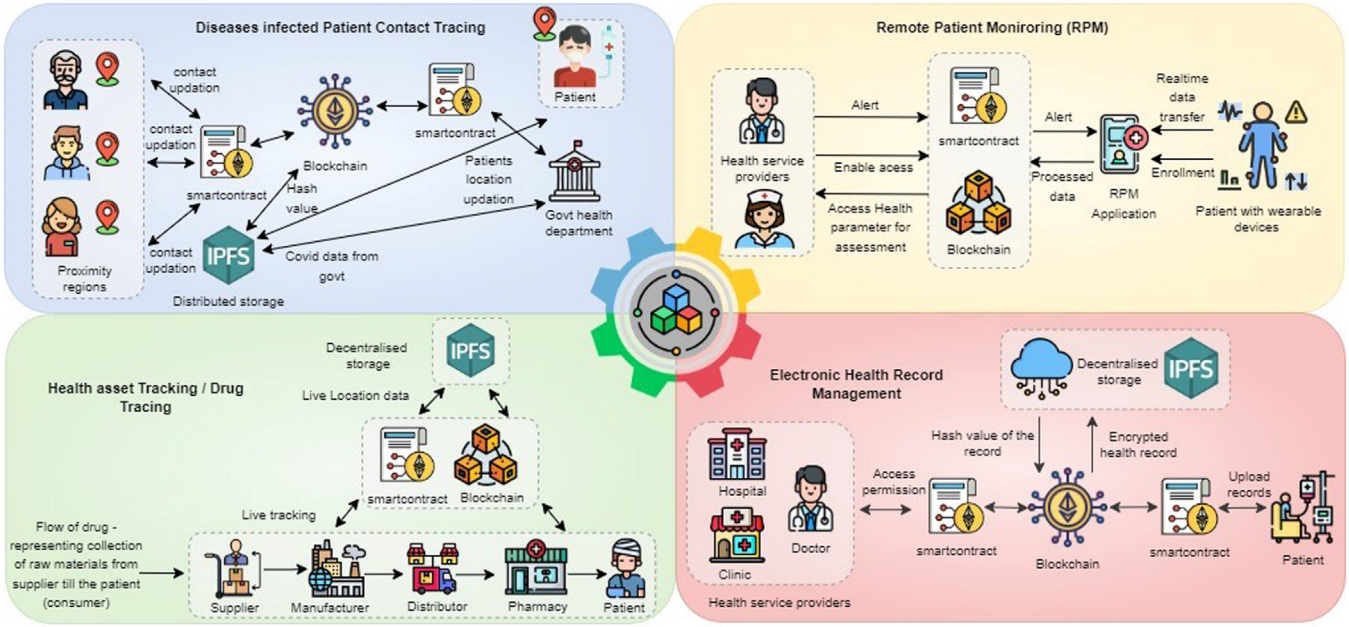


Fig. 5. BCIoT Usecases in healthcare.

allows developers to restrict the visibility of transaction by allowing only to a certain group of participants *via* smart contracts and allows only an authorized users those are mentioned in the smart contract to join the network. During the transaction evaluation process Quorum utilizes the Raft and Istanbul BFT (IBFT) consensus algorithm (Moniz, 2020) hence the overall performance of the Blockchain will be more compared to the Ethereum. Because of the unique features and characteristics of Quorum it can be used in applications of different domains which require the high speed transactions and high throughput. Quorum supports the development of collaborative environment among multiple entities (Kuo & Pham, 2023). PharmaLedger, a Quorum blockchain-based platform is developed to maintain Digital Trust Ecosystem among the various entities of pharma industry (Balan et al., 2022). Quorum Blockchain Network can also be integrated with IPFS to maintain the security of data in an IoT environment (Balakumar & Kavitha, 2021).

3.4. Multichain

Multichain is an open source private blockchain deployment platform for both private as well as consortium type of blockchain deployment supporting various operating systems such as Windows, Linux, Mac (Multichain, 2023). Multichain is a lightweight system, which exhibits three main features: (1) Ensures secure mining process without traditional PoW, (2) ensures the activities that are happening in the blockchain are visible only to a specific set of participants, (3) provision of controls over the transactions. Multichain is an extension of Bitcoin, however, the node and the wallet are two major components of helps to track the status of the chain and transactions in Multichain network. However the Multichain 1.0 version does not support complex logics in blockchain, since it doesn't support smart contracts but the Multichain 2.0 introduces smart filters for designing customized transaction validation procedures. Multichain provides a set of API's and command line interface to work with the Blockchain network. Multichain provides the flexibility to alter the IoT security configuration and permission options to the developers. SynergyChain a multichain based framework for secure data sharing with data access policies (Chang et al., 2021). To manage the health data generated from the IoT devices a multichain based model eHealthChain was developed (Pawar et al., 2022). Multichain based healthcare applications ensure the trusted and secure communication by maintaining the Confidentiality, Integrity, and Availability of Data in IoMT systems (Bhattacharjya et al., 2022).

3.5. Lessons learned

The Blockchain platforms are the key entry point for the development of any blockchain based applications. However, the diverse blockchain based platforms enables developer to test and deploy various real-time applications by providing blockchain specific features to merge with other technology. Most of the blockchain based platforms are designed to solve a specific task or problem. In our study we have discussed the features of generic platforms and their applicability in healthcare applications. Platforms nullify the unnecessary barriers during the process of development and deployment, hence platforms should be considered based on the requirement of the applications.

4. Healthcare applications

Healthcare is an essential part of every individual and over the several years, healthcare services providers are successful in providing efficient, patient-friendly medical services to the community with the aid technologies. In this section, we will discuss the integration in resolving various issues and their limitations. Fig. 5 represents the general working model of selected services using BCIoT service. Similarly Tables 5 and 6 depict the summary of existing solutions for the aforementioned applications. Existing medical services such as Remote Patient monitoring, Electronic record Management, COVID-19 infected Patient Contact tracking/tracing, and Health Asset Tracking / Drug Tracing offered by the healthcare domain by highlighting the role of BCIoT

4.1. BCIoT for Remote Patient Monitoring (RPM)

BCIoT for Remote Patient Monitoring (RPM): Over the few years, Healthcare sector has evolved by upgrading the traditional services through incorporating recent technologies. Remote Patient Monitoring is an advanced, sophisticated, technology dependent, patient friendly mode of delivering medical service aiming to benefit both patients and medical service provider. RPM is a process in which, the medical authorities or the doctors will monitor the status of a patients from a remote location using the health monitoring equipments. The patients are

Table 5
Summary of existing BCIoT based solutions for RPM and EHR management in healthcare.

Applications	Refs.	Blockchain Type	Blockchain Platform	Consensus Algorithm	Issues resolved	Contributions / Features	Limitations
RPM	(Ali et al., 2020)	Public	Ethereum	PoA (Proof-of-Authority)	Privacy and Scalability	-Tor service and Ricochet protocol, Off-chain data delivery.	-Accuracy of the system is not analysed with the existing Ethereum based RPM applications.
	(Cheikhrouhou et al., 2023)	Private	Hyperledger Fabric	Lightweight Consensus	Privacy and security of data	-Modified Blockhain Structure: Local chain within IoT layer and Global chain in Cloud layer -Novel lightweight consensus with fog nodes	-Increased number of blockchain will induces delay and decreases the overall performance.
	(Kazmi et al., 2020)	Private	Ethereum	Not specified	Data Security and Device Authentication	-Blockchain based smart contract with IoT authorization and IPFS	-Doesn't suit for large amount of Data.
	(Pradhan et al., 2021)	Consortium	Ethereum and Hyperledger	Not specified	Data Security	- Solidity based smart contract to monitor the patients based on the real-time health parameters	-The model induces the computational load as the number of data increases.
EHR Management	(Azbeg et al., 2022b)	Private	Ethereum	PoA	Security, Scalability	-Proxy re-encryption and IPFS based record management to ensure Confidentiality, integrity, privacy, access control.	- Accuracy of the model is not analysed properly with the existing models considering various parameters.
	(Zaabar et al., 2021b)	Private	Hyperledger fabric	PBFT	Data Security and Privacy	-Decentralized database to store medical data using Orbitdb and IPFS.	-Framework can be improved by considering interoperability issues.
	(Ray et al., 2021)	Private	GnuPG	Not specified	Privacy and security of Healthcare data	-Bi-layered system with swarm exchange Method.	- Model works only for small network.
	(Nishi et al., 2022)	Private	Ethereum	PoW and PoA	Secure and authorized access of data	-Hybrid smart contract based EHR Management.	Security based policies need to be implemented and analysed.

implanted with body sensors or e-Health sensors to collect the physiological data in real-time, later the collected data will be transmitted through a communication channel to the healthcare providers for further analysis.

Over the last few years, the RPM has gained the interest of many patients, who are not able to visit the hospital frequently and also during COVID-19 pandemic to avoid the risk of spreading of coronavirus. During pandemic, many healthcare providers have adopted RPM to track coronavirus and non-coronavirus patients' health conditions remotely by providing devices such as glucose monitors, digital blood pressure monitor, Pulse-oximeter. Ali et al. (2020) has proposed a Blockchain based model for sharing patient's health data to doctors without the intervention of any third-party entities in a RPM application. The model is designed using Ethereum platform with Tor service for off-chain data transfer. Even though the RPM provides an efficient medical services to patients but maintaining data security and patients privacy is a major concern. However the authors Cheikhrouhou et al. (2023) has proposed a Lightweight Blockchain-based and Fog-enabled model to provide enhanced security and response time during the data transmission in RPM systems with resource constrained IoT devices. Fog computing has escalated the responsiveness of the system by 40%.

To protect and manage the IoT device generated personal data of various patients in RPM environment, the Pham et al. (2018) has proposed Blockchain based smart contract using Ethereum where a sensed data is written automatically to the blockchain using filters to reduce the blockchain size, if the abnormalities are identified while processing, then the immediate health emergency notification will be sent to the medical service providers or Doctors. Similarly the authors, Kazmi et al. (2020) have proposed Blockchain based smart contract for authorizing the IoT sensors or the devices that are used in the RPM system. Their proposed model will improve the trust and reduces the privacy leak. Pradhan et al. (2021) has introduced a smartcontract-based RPM system for secure data transmission from and to the sensors transactions for future analysis. Similarly Wadud et al. (2020) designed a decentralized private blockchain based remote patient monitoring model with enhanced privacy and security using Patient Centric Agent (PCA) and hybrid consensus algorithm. Even though the many researchers have proposed blockhain based IoT models considering various aspects of RPM such as security of data during the transmission, privacy of data, integrity of data, response time but designing an efficient blockchain based IoT framework aimed to resolve all the existing risks is a challenging task.

4.2. BCIoT for electronic health record management

The digital revolutionization in healthcare industry has enormously increased the collection of EHR, however ensuring security of health data and privacy of patients is a challenging task using existing traditional central storage architecture and the traditional security and privacy protocols. Considering these aspects of the Healthcare domain, the authors Azbeg et al. (2022b) has proposed a secure Healthcare system by integrating Blockchain and IoT – BlockMedCare aiming to support chronic diabetic patient monitoring remotely, interns of security, scalability and processing time using proxy re-encryption technique to store hash of the data, smart contract for access control, IPFC based off-chain database to store data and Proof of Authority consensus mechanism to improve the storage process. Zaabar et al. (2021b) has proposed decentralized database architecture using Hyperledger composer to store patients' health records through OrbitDB with Interplanetary File System (IPFS). More interestingly, the authors Ray et al. (2021) has proposed a Blockchain-assisted swarm framework for timely management of EHR

Table 6
Summary of existing BCIoT based solutions for patient contact tracking and health asset tracing in healthcare.

Applications	Refs.	Blockchain Type	Blockchain Platform	Consensus Algorithm	Issues resolved	Contributions / Features	Limitations
Patient Contact tracking	(Marbouh et al., 2020)	Public	Ethereum	PoW	Data integrity and security	- Reputation contracts for assigning reputation scores – Trust analysis.	-Scalability and inter-operability of the system is not analyzed.
	(Sheeraz et al., 2021)	Not specified	Not specified	Not specified	Security and Privacy	-Model consists of 2 phases: prediction data collection, verification and tracing of infected patients and their interactions with others.	- Only theoretical approach and proper implementation is required for further analysis.
	(Rashid et al., 2022)	Private	Ethereum	PoI	Privacy and security	- Model consists of 4 components: User, Ethereum Blockchain with 2 smart contracts, Healthcare centres, Decentralized Blockchain oracles for connection	Transaction verification time is more.
	(Alsahli et al., 2021)	Private	Not specified	Not specified	Privacy, security and To reduce Power consumption	-Automated system to recognize the patients *via* interaction with authorities.	- Model works only for fixed,preselected positions/ locations.
	(Torky et al., 2021)	Not specified	Not specified	Not specified	Privacy	-Model consists of 4 components: infection verifier subsystem, surveillance system, mobile application, blockchain platform.	- Optimal results are obtained with in the specified proximity region only.
Health Asset Tracing	(Bandhu et al., 2022)	Public	Ethereum	PoW	Security, Integrity of data	-Smart contracts are developed using solidity	-Consumes more gas, energy and transaction processing time.
	(Nanda et al., 2023)	Public	Ethereum	PoW	Security, Privacy, visibility and trust.	-Major components are: ethereum network, HTTP server, PostgreSQL2 Data base, IoT devices	-System is not analysed considering the resource utilization, throughput.
	(Musamih et al., 2021)	Public	Ethereum	PoW	Security, Traceability	-Solidity language based smart contracts between actors such as Lot seller, Buyer,	-Scalability and interoperability of the system is very low.

sent through IoT ensuring secure and reliable data transfer. Their model results in better performance compare to the existing models.

To provide the secure distributed authorized access to the sensitive health records the authors Frikha et al. (2021) has designed an IoT integrated low powered Ethereum blockchain based platform. The patients, medical and paramedical entities can use their web-based or mobile-based application to retrieve the health information without any hindrance. The platform can be further enhanced by incorporating more wide range of sensors and wearable's along with the second level of encryption techniques for enhanced security. At present, we have various EHR management systems, designed considering numerous aspects but developing a reliable system by ensuring data integrity, data interoperability is a major concern while collecting data from multiple or different EHRs. However the Alamri et al. (2021) has proposed an Electronic Health Wallet (EHW) using decentralized blockchain and IPFS technologies by incorporating interoperability standards for IoT based personal health record systems (PHR). Even though the organizations and researchers have proposed many EHR models for the better management of health records while considering the records from single or multiple sources, the models further requires improvement while deploying in full-fledged working environment

4.3. BCIoT for COVID-19 infected patient contact tracking/tracing

The COVID-19 pandemic has changed the perspective of Healthcare sector due to various imposed restrictions, lack of vaccines and shortage of medical service aids at the hospitals or health centres, have not only by increased the demand for technology based medical services such as online or remote medical services *via* telemedicine, remote patient monitoring but also encouraged many researchers to develop systems for tracking the activity of infected patients, tracing contacts of patients etc. But while tracing or tracking the activities of the patients, maintaining the privacy of patient's identity is a challenging task by ensuring the policies of the healthcare department. Using the data generated by the government and healthcare department, the authors Marbouh et al. (2020) has proposed a Blockchain-based COVID-19 infected patient tracking system using ethereum smart contract and oracles. The proposed model is generic and it can be applied to any disease. Their model is tested using public blockchain network and the following observations are noted: model can process only a limited number of transactions. More interestingly, Sheeraz et al. (2021) has proposed a COVID-19 contact tracing model using Blockchain, AI and IoT technologies, where the smartwatch is used to collect the activities of the users, every transactions are recorded in the blockchain and smart contracts will enforce the access rights for end-users based on the roles and finally the machine learning models are used for predicting the COVID 19 based on the activities of the user and also for identifying the hotspots.

Torky et al. (2021) has designed a contact tracing system (CCTS) framework to verify,track, and newcases of COVID-19 with 4 components such as an infection verifier component, a mass surveillance component, a Peer to Peer mobile application, and a blockchain platform for transaction management among three components. Their model is tested in an ethereum blockchain network. Likewise, to monitor and track the informations of the COVID-19 infected patients, a Software-Defined Networking Controller (SDNC) centric public platform (Jung & Agulto, 2020) is designed. Virtual IoT (vIoT) node of the SDNC will track

Table 7
Summary of challenges and future directions.

Challenge	Description	Possible Solutions	Future Directions
Cyber Security Risks	-Patients sensitive information are collected and stored in the BCIoT system. - It is necessary to consider both Blockchain and IoT related security risk.	-Usage of Co-operative jamming strategy.	- Designing an adaptable and dynamic security frameworks that suits for both IoT and Blockchain considering the aspects of Health- care.
Privacy Risks	-In a public blockchain the transactions are visible to everyone in the network hence it is not safe for sensitive data. -Identity certification is another concern in IoT	-Use of private and permissioned Blockchain -Use of Iden- tity Management systems and automatic authentication system for IoT as well as for users. -Use of emerging cryptographic techniques such as zero-knowledge Proving, k-anonymity, differential privacy	- Use of federated Learning based blockchain to strengthen the privacy aspects.
Resource Limitations	- Increased size of blockchain. - IoT devices used in the health- care applications are equipped with minimal resources. - The Blockchain requires huge resources and computational capability	- Use of permissioned blockchain and energy efficient consensus al- gorithm. - Use of Cloud computing and Fog computing to reduce the computa tion load.	- Design of the Lightweight Blockchain that is suitable for IoT
Managing Storage Capacity	-Massive amount of patient data being collected /received by the IoT devices need to be processed/ stored. - Every transaction that is being processed are stored in the Blockchain	- Usage of off-chain based techniques for additional storage. - Usage of IPFS.	- Integration of Cloud computing with BCIoT architecture to store patient's records.
Energy Consumption	- The two major factors for high energy consumption are Mining and P2P communication.	- Alternate to PoW such as POS, PoC, PBFT - Alternative to SHA - 256 hashing algorithm Scrypt X11, and Blacke256.	- Green consensus- algorithm (Energyefficient) and Light Blockchain/Mini Blockchain

the infected or suspected individuals; hence it is responsible for updating the details in SDNC platform. Further the model accuracy can increase by incorporating intelligent search algorithm. During pandemic along with the tracking of infected patients in various part of the country, tracking the individuals who have taken/not taken the various dosages of vaccinations will be another challenging task; however the authors, Rashid et al. (2022) have proposed blockchain-based model allowing COVID-19 vaccine- and test-takers to confirm whether that person is vaccinated or not. The model also includes the contact tracing facility to alert the individuals when they are in contact with infected person. The model doesn't deal with the cyber security threats.

4.4. BCIoT for health asset tracking / drug tracing

Healthcare supply chain management system plays a major role Healthcare sector while transporting the health assets/products such as surgical, medical, and pharmaceutical items from manufacturers to the end-users. Recent decades the Healthcare supply chain management systems are facing a lot of issues, hence the use of Blockchain and IoT has the capability to establish a trust and collaborative environment for supply chain (Liu et al., 2021). IoT based blockchain technologies not only resolve the counterfeit drugs issues in supply chain but also provide privacy and reduces the theft and diversion (Ahmadi et al., 2020). Bandhu et al. (2022) has proposed a Ethereum blockchain based model for tracing and tracking of drugs in healthcare supply chain systems. QR based secure authentication method between the buyer and seller will make the system more secure, robust and reliable. Similarly the authors, Nanda et al. (2023) has proposed NAIBHSC framework using integrating blockhain and IoT with Bi-objective mathematical model to reduce the destination cost. NAIBHSC is tested using Ethereum blockhain network. Another efficient Ethereum based healthcare supply chain model for medical product tracking with off-chain storage uses smart contract based policies to provide data provenance and to eliminate the intermediaries involved during the process (Musamih et al., 2021).

4.5. Lessons learned

The Healthcare applications that are considered for the study are aimed to resolve a specific task and every application has its own requirements and critical threats, hence, to fulfill the needs, authors have used IoT and Blockhain technology is various aspects. Even though the authors/researchers are successful in achieving the task by designing a Blockchain and IoT based solutions, but they still suffer from several drawbacks. Based on the limitations of the applications it is clear that, still there is a scope for improvement in various aspects of Blockchain and IoT integration. Hence, to develop an efficient BCIoT based healthcare applications, requires a proper analysis by identifying the major challenges.

5. Challenges and open issues

Even though the Blockchain and IoT are used in various applications of Healthcare to deliver an efficient and accurate services, because their design properties and features, integration may cause additional overhead to the system. Hence from our extensive literature review, we have identified the following key challenges of the BCIoT systems in healthcare domain and also represented in Fig. 6. Additionally we have also summarized the challenges, existing solution and future enhancement options for BCIoT based systems in Table 7.

5.1. Data security

IoT devices in smart healthcare systems mostly concerned with patient's sensitive information related to current health status. Integrating Blockchain and IoT for healthcare application will resolve most of the security issues of IoT technology by embedding cryptographic techniques, to a certain level but security are still a major concern. However the distributed, heterogeneous wearable IoT devices or sensors enforce us to trust them blindly, but during the sensing process, the IoT devices may gather malicious data then the same data will be stored in the Blockchain resulting in loss of patient's sensitive data. Even though the Blockchain ensures data security in the network but the IoT components are exposed to data breach and data exploitation at the physical level. In addition to this due to increased demand for the deployment of remote patient monitoring systems, wireless networks creates additional security breaches in the Blockchain IoT environment such as replay attack, jamming, eavesdropping (Dai et al., 2019). In Blockchain based network will allow patients or medical service providers to share

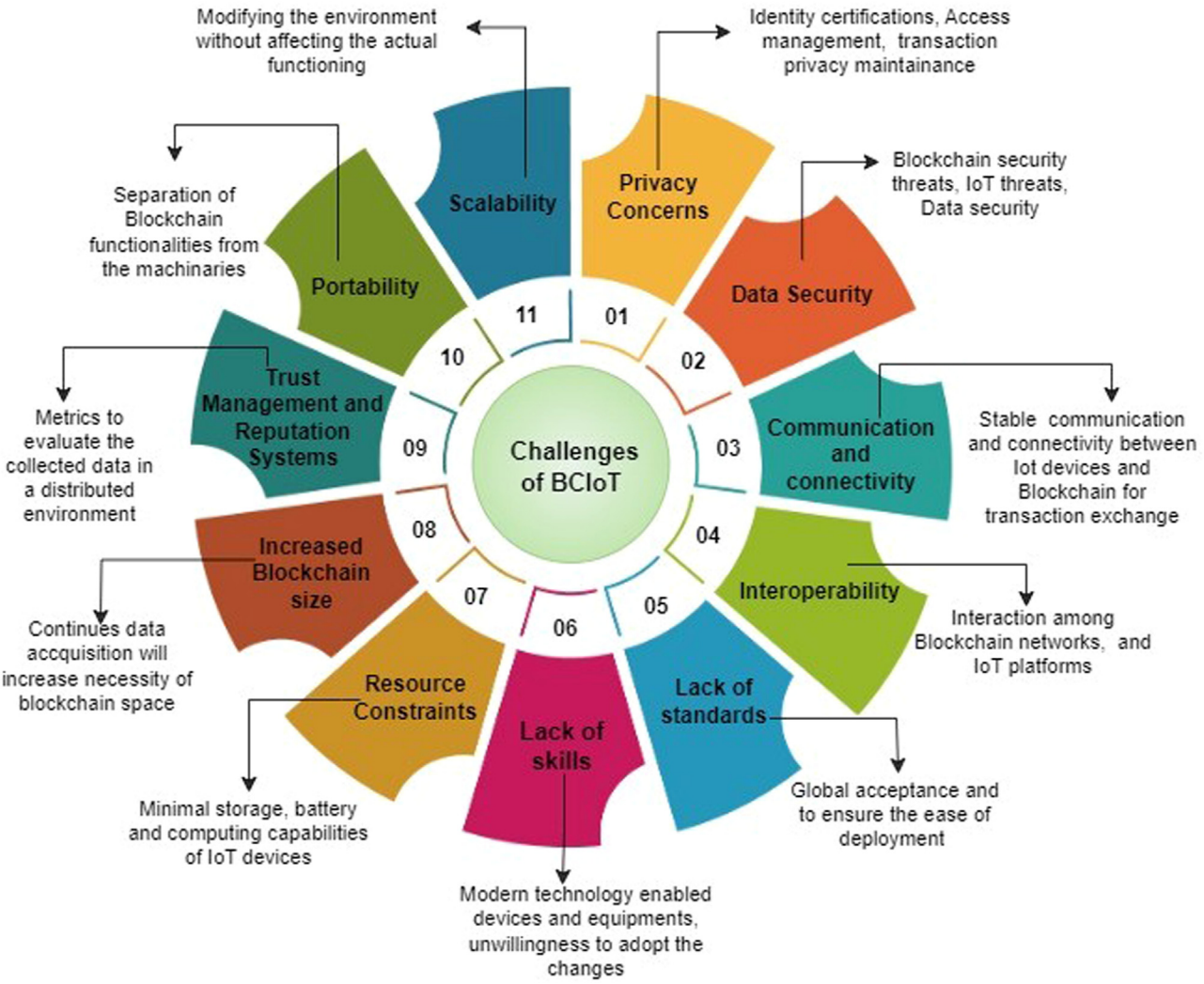


Fig. 6. Challenges of BCIoT system in healthcare.

data with securely with unknown peers but in some cases if 51% of the consensus nodes become malicious then blockchain won't be able to recognize the attack hence the patients or the authorities will not trust the unknown during data sharing activity. Along with the IoT security challenges, the authorities need to consider the Blockchain security threats such as Eclipse Attack, Sybil Attack, and Routing Attack (Nguyen et al., 2020). The deployment of efficient intrusion detection and prevention mechanism will nullify the certain attacks at the initial stages which reduce the major impact on the healthcare system.

5.2. Privacy concerns

Even though the Blockchain maintains the anonymity of the users but the transactions related to the individual patients will be executed and a copy of the same is shared among the peers through a public Blockchain channel, however, by analysing the shared details of transactions attacker can identify the IoT nodes resulting in major privacy leakage. Hence the Private Blockchain or the consortium Blockchain are most suited for sharing the sensitive data which reperents the current status of the patients among Doctors and other Medical authorities by maintaining the privacy of individuals, adopting various privacy policies. In BCIoT based Healthcare applications the IoT sensors or the IoT devices with minimal resources and computational capability are the major contributors for collecting raw data from various sources, however achieving privacy in IoT environment in terms of Identity certifications, Access management, maintaining the transaction privacy is a major concerns. The existing privacy preserving methods are inefficient and do not suit for BCIoT environment, however the modern privacy preserving mechanisms with the blend of other technologies such as homomorphic encryption (Praveen & Pabitha, 2023), ring signatures (Lai et al., 2022) and zero-knowledge proving techniques (Zhu et al., 2023) are necessary.

5.3. Interoperability

Interoperability in BCIoT based Healthcare applications are the ability to establish a smooth interaction with the different Blockchain networks and platforms involving diverse IoT sensors, storage and network components while sharing the health data among the other organizations or medical service providers without affecting the normal operations. As the adoption of IoT and Blockchain increases in healthcare domains, the interoperability becomes a fundamental concern, because the application itself consists of heterogeneous components with varied communication and connection requirement, hence the hustle free transfer of health records and other information by coordinating with all the components to provide the proper treatment to the patients is the major concern. The delay in interaction, loss of data, and loss of data integrity during the transfer or communication will cause major impact on the life of the patient. Existing solutions such as the development of common service layer - through which all the transactions, data ex-

change operations will happen irrespective of the device and platform, development of an open source framework will reduce the interoperability issues to certain extent (Villarreal et al., 2023).

5.4. Scalability

Scalability refers to the ability of a system to adapt the changes while adding or removing a component by ensuring the normal functionalities without affecting the performance. Basically, throughput is used to measure of scalability of the system i.e. the number transactions being processed in the Blockchain per second. In healthcare domain achieving scalability is a challenging task since the ecosystem consists of enormous IoT devices with Blockchain technologies, makes the system more complex interns of inducing high bandwidth overhead, demanding high computing power from resource constrained IoT devices, increases communication overhead. Hence, there exists two different approaches to improve the scalability of BCIoT i.e. on-chain and off-chain methods (Jolfaei et al., 2021). On-chain approach includes employing a modified consensus algorithms, Parallel blockchain extension, DAG-based distributed ledger (Cullen et al., 2020) and sharding techniques (Khan et al., 2021) can be used to improve the scalability of the BCIoT systems. In sharding method, rather than considering the entire system as a whole, group the IoT devices into multiple shards and finally combine the outcome of individual shards to get the final result. Similarly off-chain approaches such as side chain related works such as Ouroboros (David et al., 2018) and Algorandcan (Gilad et al., 2017) be incorporated with BCIoT to improve the scalability of the system.

5.5. Resource constraints

The most of the IoT devices possess limited resources interns of storage, computing capability, low battery power, poor network connecting capability. However the consensus mechanism used in the decentralized ledger technology requires huge computational capability, resources and consumes a lot of energy. Similarly, the IoT devices in Healthcare applications generate enormous data, However the existing Blockchain Technology drains all the available resources of the IoT devices hence to strengthen the BCIoT architecture by adopting Mobile Edge Computing (MEC) and Cloud Technologies where the IoT devices are treated as lightweight nodes to store only the hash of a blockchain data and Cloud server or the MEC server will store the entire blockchain data (Atlam et al., 2020; Chai et al., 2023).

5.6. Lack of standardization and legal issues

Although the Blockchain is still under the development stage, considering the features of Blockchain many realistic applications are being developed along with other technologies such as IoT in Healthcare and Pharmacy sectors. The lack of standards and legal regulations of Blockchain will result in imbalance of the ecosystem. The existing standard organizations need to provide well authenticated standards for various types of Blockchain as well as different ways to merge modern and existing technologies. Since the Blockchain and IoT is being adopted in Healthcare sector, where the security, privacy, trusts and traceability is maintained only by standardizing the protocols and technologies. Aspects such as - what data, size, and format can be sent to the Blockchain, and what data can be stored in the Blockchain is very much necessary, how to share the patients sensitive information collected through IoT devices (Nguyen et al., 2020).

5.7. Lack of skills among doctors and medical practitioners

It may be quite difficult to ask doctors and other medical professionals to switch from paper to technology i.e. Doctors has to use electronic records and prescriptions instead of paper. For instance, while filling out a document in their daily practise, doctors typically omit the unneeded fields. Doctors are unable to delete the information designated as required in electronic records, nevertheless. The accuracy, efficiency, and performance of technology-driven healthcare will depend on physicians' abilities and training, and depending on technologies like Blockchain and IoT for remote monitoring or other treatments might cause concern among many doctors about their accuracy and efficiency (Ratta et al., 2021).

5.8. Rapid increase in Blockchain size

Due to real-time data collection by the IoT devices or sensors in Healthcare domain such as Electronic Health Record (EHR) and Remote Patient Monitoring, the number of transactions that are being processes in the Blockchain network will massively increase. Although we can accommodate user transactions through increasing the Blockchain size by adding more number of the Blocks to the network resulting in complex system and also requires powerful mining nodes with huge resources, increased bandwidth consumption, processing time, and demands extra storage, extra computational load. Many researchers have proposed Cloud based and Fog based approaches to reduce the computational burden of IoT but it resulted in increased network latency (Nartey et al., 2021). Since most of the IoT devices that exist in the system are resource constrained by nature, hence the usage of compression methods in blockchain and also by adopting miniblockchains will resolve the current issues (Ramzan et al., 2022).

5.9. Trust management and reputation systems

Blockchain establishes a trust in the network without the need of any trusted third party entities. In Blockchain based IoT applications, most of the data being recorded through the sensors or IoT devices by sensing and observing the environment. Every decentralized BCIoT based applications consists of diversified structures, topologies, rules, constraints, transactions and communication entities produce enormous data, but the Blockchain doesn't provide any guaranteed value to establish a trust on the recorded data (Dedeoglu et al., 2020). Sharing accurate and authentic information among the nodes can be achieved by establishing a trust based network, where the node has to communicate reasonable amount of time. For a decentralized BCIoT based systems recommendation and reputation systems need to be considered for the better analysis (Ahmad et al., 2019).

5.10. Data communication and connectivity

In every healthcare application, for an instance, a remote patient monitoring (RPM) system consists of enormous IoT sensors/devices for continuous recording of the health parameters of the patients in a remote location. In every interval the device has to send the recording data to the healthcare providers, hence the RPM system has to maintain a stable connectivity with the healthcare provider to perform a secure communications without any delay or loss. It is been observed that, in a peer to peer blockchain network all the nodes are connected to a network and operate through a standard protocol but the geographically distributed, resource-constrained IoT devices are more prone vulnerabilities. To achieve the data integrity *via* secure communications mode with a stable connectivity between the devices and the blockhain few authors have proposed 5G based communication models for BCIoT (Sandeep et al., 2022). Similarly by deploying hybrid routing mechanism with efficient broadcast mitigation techniques will resolve the issues to some extent (Dammak et al., 2022).

5.11. Portability

Due to the extremely specialized nature of the protocols used in blockchain transaction operations, such as computationally intensive, thread-blocking, and time-consuming. However, it will be difficult to

deploy and manage blockchain with the majority of current industrial equipment by ensuring all the capabilities without any hindrance. Hence it is necessary to design a system which separates the operations of the blockhain from the basic functionalities and operations of the machineries (Alkhateeb et al., 2022).

6. Future directions

In this section, we have highlighted the possible future research directions to strengthen the current models by incorporating it with diversified modern technologies, aiming to provide efficient healthcare services to the patients. The various approaches are proposed based on the advantages of emerging technologies in resolving the issues and their compatibility with the existing models BCIoT based healthcare applications in various aspects of improving Quality of Life.

6.1. Light-weight Blockchain

Healthcare data Management is a process where the patience's health record are stored and managed to provide improved care by efficiently tracking the diseases and their causes. Also, the Medical data related to every patient will contribute for the development of an effective drug and efficient preventive plan. Hence to provide proper medical diagnosis using the modern technology by ensuring the security, privacy and establishing the trust among the medical stakeholders are very much necessary in the current situation (Adere, 2022). Considering the advantages of Blockchain to resolve issues of IoT in healthcare sector, the amalgamation of both requires the development of Ligtweight Model of Blockchain (Stefanescu et al., 2022) with lightweight cryptography techniques (Pal, 2023), lightweight consensus algorithm (Na & Park, 2021) with minimal resource and energy consumption, faster transaction processing.

6.2. AI enabled BCIoT

The healthcare industry is relying on technologies for their routine operations however in order to provide accurate and significant patient care and administrative procedures, the healthcare sector requires intelligent and predictive services. The enormous data being generated by the IoT devices communication through various sources requires necessary administration and improvisation. The amalgamation of AI technology with the existing BCIoT based Healthcare systems will improve the data analysis and decision making process with minimal amount of time. By employing AI technologies such as Federated Learning in BCIoT ecosystem to provide improvised, accurate and efficient healthcare services to the patients, suffering from chronic diseases by ensuring data privacy and security of health records (Rehman et al., 2022). However, the Federated learning models allows patients to participate in the learning process without sharing their local data; hence the patients need not worry about the privacy of the data (Aich et al., 2022).

6.3. 6G enabled BCIoT

6G is a promising, intelligent communication technology which enables digitization, mobilization and automation by integrating heterogeneous devices and networks by discarding the geographical boundaries. The 6G technology ensure high Quality of Life in healthcare sector by connecting all the devices and equipment's to internet which helps in improving the QoS, accuracy, efficiency of various medical services such as monitoring the patient health status from a remote location, disease diagnosis, telesurgery, intelligent accident detection, intelligent wearable's (Qadir et al., 2022). For instance the MRI and CT scanner devices will send the scanned reports to remote doctors *via* internet, for further diagnosis without any delay. 6G also reduce the existing communication and data transfer issues of BCIoT systems using terahertz (THz) signal transmission and intelligent driven devices capable of making decisions, predictions, and communicating with other devices in the network, which helps to improve the bandwidth and data, hence the overall performance of the entire system will be improved without any delay and data loss (Nguyen et al., 2021).

6.4. Quantum computing enabled BCIoT

Quantum computing has changed the traditional computing system by introducing the high speed, efficiency and reliability which intern improves the overall performance of the system. Hence the Quantum computing is suitable for applications which required huge amount of computations such as healthcare services involving a large network of connected IoT devices and Cloud *via* internet. Quantum computing is a promising technology for BCIoT based healthcare application where the doctors need to perform the real-time quick decisions based on the health conditions of the patients without any delay. Quantum computing strengthens the medical services in several ways such as enhancing the speed of diagnosis and treatment by improving the computational speed of the system, provided high level of privacy for healthcare data (Rasool et al., 2023).

6.5. Software defined networking (SDN) enabled BCIoT

SDN is promising technology for the efficient management of network operations by separating the data layer and control layer. SDN is suitable for dynamic networks, which has the capabilities to improve the scalability, confidentiality and stability of the IoT environment. The recent research works have shown that the combination of Blockchain and SDN can result in a scalable, flexibly managed infrastructure, able to interact with huge IoT devices by mitigating single point of failure and allowing devices to work in a secure, distributed environment (Turner et al., 2023). Hence, an autonomous trust mechanism for establishing the authenticity of communication between the SDN and BCIoT will strengthen the Healthcare application.

6.6. Hybrid distributed Blockchain for BCIoT

One of the major concerns in every IoT based systems are resource constrained IoT devices. To reduce the additional burden on these IoT devices we need to design a hybrid decentralized blockchain considering the various parameters such as scalability, confidentiality, throughput and latency. To protect privacy of the sensitive data and to establish an effective communication among the several IoT devices and other blockchain networks it is necessary to incorporate new strategy for interoperability and privacy preserving while designing a Hybrid Blockchain. Hence designing a hybrid blockchain will not only resolve the major issues of BCIoT but it will provide a common platform for the several IoT applications with guaranteed performance (Alkhateeb et al., 2022).

7. Conclusions

The research article presents an extensive survey on the integration of IoT and Blockchain technologies for healthcare domain. At the beginning, the impacts of modern technologies such as IoT and Blockchain in medical services are discussed. Later a detailed overview of the IoT and Blockchain technologies with architectural components, working, characteristics, challenges, and various BCIoT integration options along with the existing healthcare applications with BCIoT architecture are discussed. Then, the various enabling platforms for the amalgamation are discussed followed by the discussion on the various potential applications of BCIoT in healthcare such as Remote patient monitoring, electronic heath record management, drug tracing, disease infected patient contact tracing. Moreover the article highlights the different integration challenges of BCIoT in Healthcare with existing solutions and

finally with a proper analysis, possible future directions and advancement options are recommended to strengthen the BCIoT architecture for Healthcare services.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Abdellatif, A. A., Samara, L., Mohamed, A., Erbad, A., Chiasserini, C. F., Guizani, M., et al., (2021). Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange. *IEEE Internet of Things Journal, 8*(21), 15762–15775.

Abutaleb, R. A., Alqahtany, S. S., & Syed, T. A. (2023). Integrity and privacy-aware, patient-centric health record access control framework using a blockchain. *Applied Sciences, 13*(2), 1028.

Adere, E. M. (2022). Blockchain in healthcare and IoT: A systematic literature review. *Array, 1*, 100139.

Ahmad, F., Ahmad, Z., Kerrache, C. A., Kurugollu, F., Adnane, A., & Barka, E. (2019). Blockchain in internet-of-things: Architecture, applications and research directions. In *Proceedings of the 2019 international conference on computer and information sciences (ICCIS)* (pp. 1–6). IEEE.

Ahmadi, V., Benjelloun, S., El Kik, M., Sharma, T., Chi, H., & Zhou, W. (2020). Drug governance: Iot-based blockchain implementation in the pharmaceutical supply chain. In *Proceedings of the 2020 sixth international conference on mobile and secure services (MobiSecServ)* (pp. 1–8). IEEE.

Ahmed, I., Jeon, G., & Chehri, A. (2022). An IoT-enabled smart health care system for screening of covid-19 with multi layers features fusion and selection. *Computing*, 1–18.

Ahmed, N., Ahammed, R., Islam, M. M., Uddin, M. A., Akhter, A., Talukder, M. A., et al., (2021). Machine learning based diabetes prediction and development of smart web application. *International Journal of Cognitive Computing in Engineering, 2*, 229–241.

Aich, S., Sinai, N. K., Kumar, S., Ali, M., Choi, Y. R., Joo, M. I., et al., (2022). Protecting personal healthcare record using blockchain & federated learning technologies. In *Proceedings of the 2022 24th international conference on advanced communication technology (ICACT)* (pp. 109–112). IEEE.

Akhter Md Hasib, K. T., Chowdhury, I., Sakib, S., Monirujjaman Khan, M., Alsufyani, N., Alsufyani, A., et al., (2022). Electronic health record monitoring system and data security using Blockchain technology. *Security and Communication Networks, 2022*, 1–15.

Alaa, M., Zaidan, A. A., Zaidan, B. B., Talal, M., & Kiah, M. L. M. (2017). A review of smart home applications based on internet of things. *Journal of Network and Computer Applications, 97*, 48–65.

Alamri, B., Javed, I. T., & Margaria, T. (2021). A gdpr-compliant framework for IoT-based personal health records using blockchain. In *Proceedings of the 2021 11th IFIP international conference on new technologies, mobility and security (NTMS)* (pp. 1–5). IEEE.

Aleksic, S. (2019). A survey on optical technologies for iot, smart industry, and smart infrastructures. *Journal of Sensor and Actuator networks, 8*(3), 47.

Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). Applications of blockchains in the internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials, 21*(2), 1676–1717.

Ali, M. S., Vecchio, M., Putra, G. D., Kanhere, S. S., & Antonelli, F. (2020). A decentralized peer-to-peer remote health monitoring system. *Sensors, 20*(6), 1656.

Ali, O., Jaradat, A., Kulakli, A., & Abuhalimeh, A. (2021). A comparative study: Blockchain technology utilization benefits, challenges and functionalities. *IEEE Access : Practical Innovations, Open Solutions, 9*, 12730–12749.

Al-Joboury, I. M., & Al-Hemiary, E. H. (2021). *Automated decentralized IoT based blockchain using ethereum smart contract for healthcare," Enhanced telemedicine and e-Health: Advanced IoT enabled soft computing framework* (pp. 179–198). Springer.

Alkhateeb, A., Catal, C., Kar, G., & Mishra, A. (2022). Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review. *Sensors, 22*(4), 1304.

Alsahli, M. A., Alsanad, A., Hassan, M. M., & Gumaei, A. (2021). Privacy preservation of user identity in contact tracing for covid-19-like pandemics using edge computing. *IEEE Access : Practical Innovations, Open Solutions, 9*, 125065–125079.

Atlam, H. F., Azad, M. A., Alzahrani, A. G., & Wills, G. (2020). A review of blockchain in internet of things and ai. *Big Data and Cognitive Computing, 4*(4), 28.

Atlam, H. F., & Wills, G. B. (2019). Technical aspects of blockchain and IoT. In *Advances in computers: 115* (pp. 1–39). Elsevier.

Azbeg, K., Ouchetto, O., Andaloussi, S., & Fetjah, L. (2022a). A taxonomic review of the use of IoT and Blockchain in healthcare applications. *IRBM, 43*(5), 511–519.

Azbeg, K., Ouchetto, O., & Andaloussi, S. J. (2022b). Blockmedcare: A healthcare system based on iot, blockchain and ipfs for data management security. *Egyptian Informatics Journal, 23*(2), 329–343.

Azbeg, K., Ouchetto, O., Andaloussi, S. Jai, & Fetjah, L. (2021). An overview of blockchain consensus algorithms: Comparison, challenges and future directions. In *Advances on smart and soft computing: Proceedings of ICACIn 2020* (pp. 357–369).

Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of things for smart healthcare: Technologies, challenges, and opportunitie. *IEEE Access : Practical Innovations, Open Solutions, 5*, 26521–26544.

Balakumar, S., & Kavitha, A. R. (2021). Quorum-based blockchain network with IPFS to improve data security in IoT network. *Studies in Informatics and Control, 30*, 85–98.

Balan, A., Alboaie, S., & Rat, A. (2022). ˘a, "Pharmaledger a blockchain-enabled healthcare platform. In *Proceedings of the 2022 E-health and bioengineering conference (EHB)* (pp. 1–6). IEEE.

Bandhu, K. C., Litoriya, R., Lowanshi, P., Jindal, M., Chouhan, L., & Jain, S. (2022). Making drug supply chain secure traceable and efficient: A blockchain and smart contract based implementation. *Multimedia Tools and Applications*, 1–28.

Banotra, A., Sharma, J. S., Gupta, S., Gupta, S. K., & Rashid, M. (2021). Use of blockchain and internet of things for securing data in healthcare systems. In *Multimedia security: Algorithm development, analysis and applications* (pp. 255–267). Springer.

Beg, S., Handa, M., Shukla, R., Rahman, M., Almalki, W. H., Afzal, O., et al., (2022). Wearable smart devices in cancer diagnosis and remote clinical trial monitoring: Transforming the healthcare applications. *Drug Discovery Today, 27*.

Bhattacharjya, A., Kozdr´oj, K., Bazydło, G., & Wisniewski, R. (2022). Trusted and secure blockchain-based architecture for internet-of-medical-things. *Electronics, 11*(16), 2560.

Bhuiyan, M. N., Rahman, M. M., Billah, M. M., & Saha, D. (2021). Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet of Things Journal, 8*(13), 10474–10498.

Chai, F., Zhang, Q., Yao, H., Xin, X., Gao, R., & Guizani, M. (2023). Joint multi-task offloading and resource allocation for mobile edge computing systems in satellite IoT. *IEEE Transactions on Vehicular Technology, 72*, 7783–7795.

B. Chander and G. Kumaravelan, "Internet of things: Foundation," Principles of internet of things (IoT) ecosystem: Insight paradigm, pp. 3–33, 2020.

Chang, J., Ni, J., Xiao, J., Dai, X., & Jin, H. (2021). Synergychain: A multichain-based data-sharing framework with hierarchical access control. *IEEE Internet of Things Journal, 9*(16), 14767–14778.

Cheikhrouhou, O., Mershad, K., Jamil, F., Mahmud, R., Koubaa, A., & Moosavi, S. R. (2023). A lightweight blockchain and fog-enabled secure remote patient monitoring system. *Internet of Things*, Article 100691.

Cullen, A., Ferraro, P., King, C., & Shorten, R. (2020). On the resilience of dag-based distributed ledgers in IoT applications. *IEEE Internet of Things Journal, 7*(8), 7112–7122.

Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: A survey. *IEEE Internet of Things Journal, 6*(5), 8076–8094.

Dammak, B., Turki, M., Cheikhrouhou, S., Baklouti, M., Mars, R., & Dhahbi, A. (2022). Lorachaincare: An iot architecture integrating blockchain and lora network for personal health care data monitoring. *Sensors, 22*(4), 1497.

Dang, L. M., Piran, M. J., Han, D., Min, K., & Moon, H. (2019). A survey on internet of things and cloud computing for healthcare. *Electronics, 8*(7), 768.

David, B., Ga˘zi, P., Kiayias, A., & Russell, A. (2018). Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Proceedings of the advances in cryptology–EUROCRYPT 2018: 37th annual international conference on the theory and applications of cryptographic techniques* (pp. 66–98). Springer. April 29-May 3, 2018 Proceedings, Part II 37.

Dedeoglu, V., Jurdak, R., Dorri, A., Lunardi, R., Michelin, R., Zorzo, A., et al., (2020). Blockchain technologies for IoT. *Advanced Applications of Blockchain Technology*, 55–89.

Dewangan, N. K., & Chandrakar, P. (2022). Patient-centric token-based healthcare blockchain implementation using secure internet of medical things. *IEEE Transactions on Computational Social Systems*.

Dwivedi, R., Mehrotra, D., & Chandra, S. (2022). Potential of internet of medical things (iomt) applications in building a smart healthcare system: A systematic review. *Journal of Oral Biology and Craniofacial Research, 12*(2), 302–318.

Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications, 177*, 102936.

Farhan, L., Kharel, R., Kaiwartya, O., Quiroz-Castellanos, M., Alissa, A., & Abdulsalam, M. (2018). A concise review on internet of things (IoT)-problems, challenges and opportunities. In *Proceedings of the 2018 11th international symposium on communication systems, networks & digital signal processing (CSNDSP)* (pp. 1–6). IEEE.

Fatokun, T., Nag, A., & Sharma, S. (2021). Towards a blockchain assisted patient owned system for electronic health records. *Electronics, 10*(5), 580.

Ethereum. What is ethereum. (2023). [Online]. Available: https://ethereum.org/en/what-is-ethereum/.

Frankenfield, J. (2023) Distributed ledger technology (DLT): Definition and how it works. [Online]. Available: https://www.investopedia.com/terms/d/distributed-ledger-technology-dlt.asp.

Foundation, H. (2023). *About hyperledger foundation* [Online]. Available: https://www.hyperledger.org/about.

Frikha, T., Chaari, A., Chaabane, F., Cheikhrouhou, O., & Zaguia, A. (2021). Healthcare and fitness data management using the iot-based blockchain platform. *Journal of Healthcare Engineering, 2021*.

Gao, S. (2021). Gray level co-occurrence matrix and extreme learning machine for Alzheimer's disease diagnosis. *International Journal of Cognitive Computing in Engineering, 2*, 116–129.

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., & Zeldovich, N. (2017). Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th symposium on operating systems principles* (pp. 51–68).

Goel, P. (2022) Is blockchain the solution for failing global healthcare? [Online]. Available: https://www.weforum.org/agenda/2022/09/blockchain-solution-for-failing-global-healthcare/.

Gu, W., Li, J., & Tang, Z. (2021). A survey on consensus mechanisms for blockchain technology. In *Proceedings of the 2021 international conference on artificial intelligence, big data and algorithms (CAIBDA)* (pp. 46–49). IEEE.

Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks, 2*, 130–139.

Hathaliya, J., Sharma, P., Tanwar, S., & Gupta, R. (2019). Blockchain-based remote patient monitoring in healthcare 4.0. In *Proceedings of the 2019 IEEE 9th international conference on advanced computing (IACC)* (pp. 87–91). IEEE.

Huang, H., Sun, X., Xiao, F., Zhu, P., & Wang, W. (2021). Blockchain-based ehealth system for auditable EHRS manipulation in cloud environments. *Journal of Parallel and Distributed Computing, 148*, 46–57.

Iftekhar, A., Cui, X., Tao, Q., & Zheng, C. (2021). Hyperledger fabric access control system for internet of things layer in blockchain-based applications. *Entropy, 23*(8), 1054.

Islam, M. R., Rahman, M. M., Mahmud, M., Rahman, M. A., Mohamad, M. H. S., et al., (2021). A review on blockchain security issues and challenges. In *Proceedings of the 2021 IEEE 12th control and system graduate research colloquium (ICSGRC)* (pp. 227–232). IEEE.

Javaid, M., & Khan, I. H. (2021). Internet of things (iot) enabled healthcare helps to take the challenges of covid-19 pandemic. *Journal of Oral Biology and Craniofacial Research, 11*(2), 209–214.

Jolfaei, A. A., Aghili, S. F., & Singelee, D. (2021). A survey on blockchain-based IOMT systems: Towards scalability. *IEEE Access: Practical Innovations, Open Solutions, 9*, 148948–148975.

Jung, Y., & Agulto, R. (2020). A public platform for virtual iot-based monitoring and tracking of covid-19. *Electronics, 10*(1), 12.

Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., & Maddikunta, P. K. R. (2022). A review on security and privacy of internet of medical things. In *Intelligent internet of things for healthcare and industry* (pp. 171–187). Springer.

Kakkar, L., Gupta, D., Saxena, S., & Tanwar, S. (2021). IoT architectures and its security: A review. In *Proceedings of the second international conference on information management and machine intelligence: ICIMMI 2020* (pp. 87–94). Springer.

Kapoor, A. (2021) The impact of the internet of things on web design and development. [Online]. Available: https://theiotmagazine.com/the-impact-of-the-internet-of-things-on-web-design-and-development-c4dcef3d55f7.

Karar, M. E., Alotaibi, B., & Alotaibi, M. (2022). Intelligent medical iot-enabled automated microscopic image diagnosis of acute blood cancers. *Sensors, 22*(6), 2348.

Karunanithy, K., & Velusamy, B. (2022). Edge device based efficient data collection in smart health monitoring system using wireless body area network. *Biomedical Signal Processing and Control, 72*, Article 103280.

Kaur, S., Chaturvedi, S., Sharma, A., & Kar, J. (2021). A research survey on applications of consensus protocols in blockchain. *Security and Communication Networks, 2021*, 1–22.

Kazmi, H. S. Z., Nazeer, F., Mubarak, S., Hameed, S., Basharat, A., & Javaid, N. (2020). Trusted remote patient monitoring using blockchain-based smart contracts. In *Advances on broad-band wireless computing, communication and applications: Proceedings of the 14th international conference on broad-band wireless computing, communication and applications (BWCCA-2019) 14* (pp. 765–776). Springer.

Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. *Applied Sciences, 11*(20), 9372.

Khatri, S., Alzahrani, F. A., Ansari, M. T. J., Agrawal, A., Kumar, R., & Khan, R. A. (2021). A systematic analysis on Blockchain integration with healthcare domain: Scope and challenges. *IEEE Access: Practical Innovations, Open Solutions, 9*, 84666–84687.

Kothari, S., Tazrin, T., Desai, D., Parveen, A., Fouda, M. M., & Fadlullah, Z. M. (2021). On securing electronic healthcare records using hyperledger fabric across the network edge. In *Secure edge computing* (pp. 155–176). CRC Press.

Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2020). Security in IOMT communications: A survey. *Sensors, 20*(17), 4828.

Kumar, L. A., Renuka, D. K., Rose, S. L., Wartana, I. M., et al., (2022). Deep learning based assistive technology on audio visual speech recognition for heaing impaired. *International Journal of Cognitive Computing in Engineering, 3*, 24–30.

Kumar, M., & Chand, S. (2021). Medhypchain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in covid-19 pandemic. *Journal of Network and Computer Applications, 179*, Article 102975.

Kuo, T. T., & Pham, A. (2023). Quorum-based model learning on a blockchain hierarchical clinical research network using smart contracts. *International Journal of Medical Informatics, 169*, Article 104924.

Lai, C., Ma, Z., Guo, R., & Zheng, D. (2022). Secure medical data sharing scheme based on traceable ring signature and blockchain. *Peer-to-Peer Networking and Applications, 15*(3), 1562–1576.

Lakhan, A., Mohammed, M. A., Rashid, A. N., Kadry, S., Panityakul, T., Abdulkareem, K. H., et al., (2021). Smart-contract aware ethereum and client-fog-cloud healthcare system. *Sensors, 21*(12), 4093.

Lashkari, B., & Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. *IEEE Access: Practical Innovations, Open Solutions, 9*, 43620–43652.

Li, X., Zhai, M., & Sun, J. (2021a). Ddcnnc: Dilated and depthwise separable convolutional neural network for diagnosis covid-19 *via* chest x-ray images. *International Journal of Cognitive Computing in Engineering, 2*, 71–82.

Li, Y., Zhao, J., Lv, Z., & Li, J. (2021b). Medical image fusion method by deep learning. *International Journal of Cognitive Computing in Engineering, 2*, 21–29.

Liu, X., Barenji, A. V., Li, Z., Montreuil, B., & Huang, G. Q. (2021). Blockchain-based smart tracking and tracing platform for drug supply chain. *Computers & Industrial Engineering, 161*, Article 107669.

Lombardi, M., Pascale, F., & Santaniello, D. (2021). Internet of things: A general overview between architectures, protocols and applications. *Information, 12*(2), 87.

Madakam, S., Lake, V., Lake, V., Lake, V., et al., (2015). Internet of things (IoT): A literature review. *Journal of Computer and Communications, 3*(05), 164.

Mahmood, K., Tariq, T., Sangaiah, A. K., Ghaffar, Z., Saleem, M. A., & Shamshad, S. (2023). A neural computing-based access control protocol for AI-driven intelligent flying vehicles in industry 5.0-assisted consumer electronics. *IEEE Transactions on Consumer Electronics*.

Majumder, D. P. (2022). The study of consensus algorithms in Blockchain. In *Blockchain* (pp. 21–34). Chapman and Hall/CRC.

Malhotra, P., Singh, Y., Anand, P., Bangotra, D. K., Singh, P. K., & Hong, W. C. (2021). Internet of things: Evolution, concerns and security challenges. *Sensors, 21*(5), 1809.

Marbouh, D., Abbasi, T., Maasmi, F., Omar, I. A., Debe, M. S., Salah, K., et al., (2020). Blockchain for covid-19: Review, opportunities, and a trusted tracking system. *Arabian journal for Science and Engineering, 45*, 9895–9911.

Meshcheryakov, Y., Melman, A., Evsutin, O., Morozov, V., & Koucheryavy, Y. (2021). On performance of PBFT blockchain consensus algorithm for IoT applications with constrained devices. *IEEE Access: Practical Innovations, Open Solutions, 9*, 80559–80570.

Moniz, H. "The Istanbul BFT consensus algorithm," arXiv preprint , 2020.

Multichain. Multichain. (2023) [Online]. Available: https://www.multichain.com/.

Muralidharan, K., Ramesh, A., Rithvik, G., Prem, S., Reghunaath, A., & Gopinath, M. (2021). 1d convolution approach to human activity recognition using sensor data and comparison with machine learning algorithms. *International Journal of Cognitive Computing in Engineering, 2*, 130–143.

Musamih, A., Salah, K., Jayaraman, R., Arshad, J., Debe, M., Al-Hammadi, Y., et al., (2021). A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access: Practical Innovations, Open Solutions, 9*, 9728–9743.

Na, D., & Park, S. (2021). Fusion chain: A decentralized lightweight blockchain for iot security and privacy. *Electronics, 10*(4), 391.

Nakamoto, S. "Bitcoin: A peer-to-peer electronic cash system," Decentralized business review, p. 21260, 2008.

Nancy, A. A., Ravindran, D., Raj Vincent, P. D., Srinivasan, K., & Gutierrez Reina, D. (2022). IoT-cloud-based smart healthcare monitoring system for heart disease prediction *via* deep learning. *Electronics, 11*(15), 2292.

Nanda, S. K., Panda, S. K., & Dash, M. (2023). Medical supply chain integrated with blockchain and IoT to track the logistics of medical products. *Multimedia Tools and Applications*, 1–23.

Nartey, C., Tchao, E. T., Gadze, J. D., Keelson, E., Klogo, G. S., Kommey, B., et al., (2021). On Blockchain and IoT integration platforms: Current implementation challenges and future perspectives. *Wireless Communications and Mobile Computing, 2021*, 1–25.

Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., Niyato, D., et al., (2021). Poor, "6g internet of things: A comprehensive survey. *IEEE Internet of Things Journal, 9*(1), 359–383.

Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, applications and challenges. *IEEE Communications Surveys & Tutorials, 22*(4), 2521–2549.

Nie, X., Zhang, A., Chen, J., Qu, Y., Yu, S., et al., (2022). Time-enabled and verifiable secure search for blockchain-empowered electronic health record sharing in IoT. *Security and Communication Networks, 2022*.

Nishi, F. K., Shams-E-Mofiz, M., Khan, M. M., Alsufyani, A., Bourouis, S., Gupta, P., et al., (2022). Electronic healthcare data record security using blockchain and smart contract. *Journal of Sensors, 2022*, 1–22.

Pal, K. (2023). Blockchain with the internet of things for secure healthcare service using lightweight cryptography. In *Blockchain applications in cryptocurrency for technological evolution* (pp. 60–93). IGI Global.

Pawar, P., Parolia, N., Shinde, S., Edoh, T. O., & Singh, M. (2022). ehealthchain—A blockchain-based personal health information management system. *Annals of Telecommunications, 17*, 1–13.

Pham, H. L., Tran, T. H., & Nakashima, Y. (2018). A secure remote healthcare system for hospital using blockchain smart contract. In *Proceedings of the 2018 IEEE Globecom workshops (GC wkshps)* (pp. 1–6). IEEE.

Pradhan, N. R., Rout, S. S., & Singh, A. P. (2021). Blockchain based smart healthcare system for chronic–illness patient monitoring. In *Proceedings of the 2020 3rd international conference on energy, power and environment: Towards clean energy technologies* (pp. 1–6). IEEE.

Prasad, J., Jain, A., Velho, D., & KS, S. K. (2022). Covid vision: An integrated face mask detector and social distancing tracker. *International Journal of Cognitive Computing in Engineering, 3*, 106–113.

Prathibha, S., Hongal, A., & Jyothi, M. (2017). Iot based monitoring system in smart agriculture. In *Proceedings of the 2017 international conference on recent advances in electronics and communication technology (ICRAECT)* (pp. 81–84). IEEE.

Praveen, R., & Pabitha, P. (2023). Improved gentry–halevi's fully homomorphic encryption-based lightweight privacy preserving scheme for securing medical internet of things. *Transactions on Emerging Telecommunications Technologies, 34*, e4732.

Qadir, Z., Le, K. N., Saeed, N., & Munawar, H. S. (2022). *Towards 6g internet of things: Recent advances, use cases, and open challenges*. ICT Express.

Quorum. Build on Quorum, the complete open source blockchain platform for business. 2023 [Online]. Available: https://consensys.net/quorum/

Rahman, M. S., Islam, M. A., Uddin, M. A., & Stea, G. (2022). A survey of blockchain-based IoT ehealthcare: Applications, research issues, and challenges. *Internet of Things, 19*, Article 100551.

Ramkumar, M. P., Mano Paul, P. D., Maram, B., & Ananth, J. P. (2022). Deep maxout network for lung cancer detection using optimization algorithm in smart internet of things. *Concurrency and Computation: Practice and Experience, 34*(25), e7264.

Ramzan, S., Aqdus, A., Ravi, V., Koundal, D., Amin, R., & Al Ghamdi, M. A. (2022). Healthcare applications using blockchain technology: Motivations and challenges. *IEEE Transactions on Engineering Management, 70*, 2874–2890.

Rashid, M. M., Choi, P., Lee, S. H., & Kwon, K. R. (2022). Block-hpct: Blockchain enabled digital health passports and contact tracing of infectious diseases like covid-19. *Sensors, 22*(11), 4256.

Rasool, R. U., Ahmad, H. F., Rafique, W., Qayyum, A., Qadir, J., & Anwar, Z. (2023). Quantum computing for healthcare: A review. *Future Internet, 15*(3), 94.

Ratta, P., Kaur, A., Sharma, S., Shabaz, M., & Dhiman, G. (2021). Application of blockchain and internet of things in healthcare and medical sector: Applications, challenges, and future perspectives. *Journal of Food Quality, 2021*, 1–20.

Ray, P. P., Chowhan, B., Kumar, N., & Almogren, A. (2021). Biothr: Electronic health record servicing scheme in iot-blockchain ecosystem. *IEEE Internet of Things Journal, 8*(13), 10857–10872.

Rehman, A., Abbas, S., Khan, M., Ghazal, T. M., Adnan, K. M., & Mosavi, A. (2022). A secure healthcare 5.0 system based on Blockchain technology entangled with federated learning technique. *Computers in Biology and Medicine, 150*, Article 106019.

Sadawi, A. A., Hassan, M. S., & Ndiaye, M. (2021). A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. *IEEE Access: Practical Innovations, Open Solutions, 9*, 54478–54497.

Samizadeh Nikoui, T., Rahmani, A. M., Balador, A., & Haj Seyyed Javadi, H. (2021). Internet of things architecture challenges: A systematic review. *International Journal of Communication Systems, 34*(4), e4678.

Samuel, O., Omojo, A. B., Mohsin, S. M., Tiwari, P., Gupta, D., & Band, S. S. (2022). An anonymous IoT-based e-health monitoring system using blockchain technology. *IEEE Systems Journal, 17*, 2422–2433.

Sandeep, B., Rao, V. B., Aditya, K., Sekhar, S. M., & Siddesh, G. (2022). Blockchain-based privacy approaches for 5g healthcare informatics. In *Blockchain applications for healthcare informatics* (pp. 213–242). Elsevier.

Sangaiah, A. K., Javadpour, A., Ja'fari, F., Zavieh, H., & Khaniabadi, S. M. (2023). Sala-IoT: Self-reduced internet of things with learning automaton sleep scheduling algorithm. *IEEE Sensors Journal*.

Sanka, A. I., Irfan, M., Huang, I., & Cheung, R. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer Communications, 169*, 179–201.

Saxena, S., Bhushan, B., & Ahad, M. A. (2021). Blockchain based solutions to secure IoT: Background, integration trends and a way forward. *Journal of Network and Computer Applications, 181*, Article 103050.

ServUsTECH. 5 IoT Trends That Will Influence Innovation in 2023. [Online]. Available: https://www.linkedin.com/pulse/5-iot-trends-influence-innovation-2023-servustech.

Sethi, P., & Sarangi, S. R. (2017). Internet of things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering, 2017*.

Shammar, E. A., Zahary, A. T., & Al-Shargabi, A. A. (2021). A survey of iot and blockchain integration: Security perspective. *IEEE Access: Practical Innovations, Open Solutions, 9*, 156114–156150.

Sharma, A., Bahl, S., Bagha, A. K., Javaid, M., Shukla, D. K., & Haleem, A. (2020). Blockchain technology and its applications to combat covid-19 pandemic. *Research on Biomedical Engineering*, 1–8.

Sheeraz, M. M., Athar, A., Hussain, A., Aich, S., Joo, M. I., & Kim, H. C. (2021). Blockchain, AI & IoT based covid-19 contact tracing and distancing framework. In *Proceedings of the 2021 international conference on robotics and automation in industry (ICRAI)* (pp. 1–6). IEEE.

Srivastava, G., Crichigno, J., & Dhar, S. (2019). A light and secure healthcare blockchain for IoT medical devices. In *Proceedings of the 2019 IEEE Canadian conference of electrical and computer engineering (CCECE)* (pp. 1–5). IEEE.

Srivastava, V., Mahara, T., & Yadav, P. (2021). An analysis of the ethical challenges of blockchain-enabled e-healthcare applications in 6g networks. *International Journal of Cognitive Computing in Engineering, 2*, 171–179.

Stamatellis, C., Papadopoulos, P., Pitropakis, N., Katsikas, S., & Buchanan, W. J. (2020). A privacy-preserving healthcare framework using hyperledger fabric. *Sensors, 20*(22), 6587.

Stefanescu, D., Montalvillo, L., Gal´an-Garc´ıa, P., Unzilla, J., & Urbieta, A. (2022). *A systematic literature review of lightweight Blockchain for IoT* (pp. 123138–123159). IEEE Access.

Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences, 10*(12), 4102.

Thandapani, S., Mahaboob, M. I., Iwendi, C., Selvaraj, D., Dumka, A., Rashid, M., et al., (2023). IOMT with deep CNN: AI-based intelligent support system for pandemic diseases. *Electronics, 12*(2), 424.

Tiwari, A., Dhiman, V., Iesa, M. A., Alsarhan, H., Mehbodniya, A., Shabaz, M., et al., (2021). Patient behavioral analysis with smart healthcare and iot. *Behavioural Neurology, 2021*.

Torky, M., Goda, E., Snasel, V., & Hassanien, A. E. (2021). Covid-19 contact tracing and detection-based on Blockchain technology. In *Informatics: 8* (p. 72). Multidisciplinary Digital Publishing Institute.

Torky, M., & Hassanein, A. E. (2020). Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. *Computers and Electronics in Agriculture, 178*, Article 105476.

Turner, S. W., Karakus, M., Guler, E., & Uludag, S. (2023). A promising integration of SDN and blockchain for IoT networks: A survey. In *IEEE Access* (pp. 29800–29822).

Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2018). Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access: Practical Innovations, Open Solutions, 6*, 32700–32726.

Vermesan, O., & Friess, P. (2022). *Internet of things-global technological and societal trends from smart environments and spaces to green ICT*. CRC Press.

Villarreal, E. R. D., Garc´ıa-Alonso, J., Moguel, E., & Alegr´ıa, J. A. H. (2023). Blockchain for healthcare management systems: A survey on interoperability and security. *IEEE Access: Practical Innovations, Open Solutions, 11*, 5629–5652.

Wadud, M. A. H., Bhuiyan, T. A. U. H., Uddin, M. A., & Rahman, M. M. (2020). A patient centric agent assisted private Blockchain on hyperledger fabric for managing remote patient monitoring. In *Proceedings of the 2020 11th international conference on electrical and computer engineering (ICECE)* (pp. 194–197). IEEE.

Xie, H., Zheng, J., He, T., Wei, S., & Hu, C. (2023). Tebds: A trusted execution environment-and-blockchain-supported IoT data sharing system. *Future Generation Computer Systems, 140*, 321–330.

Xiong, H., Chen, M., Wu, C., Zhao, Y., & Yi, W. (2022). Research on progress of Blockchain consensus algorithm: A review on recent progress of blockchain consensus algorithms. *Future Internet, 14*(2), 47.

Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 1–16.

Zaabar, B., Cheikhrouhou, O., Ammi, M., Awad, A. I., & Abid, M. (2021a). Secure and privacy-aware blockchain-based remote patient monitoring system for internet of healthcare things. In *Proceedings of the 2021 17th international conference on wireless and mobile computing, networking and communications (WiMob)* (pp. 200–205). IEEE.

Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021b). Healthblock: A secure Blockchain-based healthcare data management system. *Computer Networks, 200*, Article 108500.

Zhang, C., Xu, C., Sharif, K., & Zhu, L. (2021). Privacy-preserving contact tracing in 5g-integrated and Blockchain-based medical applications. *Computer Standards & Interfaces, 77*, Article 103520.

Zhang, J., Yang, Y., Liu, X., & Ma, J. (2022). An efficient blockchain-based hierarchical data sharing for healthcare internet of things. *IEEE Transactions on Industrial Informatics, 18*(10), 7139–7150.

Zhu, J., Feng, W., Zhong, W., Huang, M., Feng, S., et al., (2023). Research on privacy protection of technology service transactions based on blockchain and zero-knowledge proof. *Wireless Communications and Mobile Computing, 2023*.