A Transformative Shift Towards Blockchain-based IoT Environments: Consensus, Smart Contracts, and Future Directions

Chandan Trivedi[1], Udai Rao[2], Keyur Parmar[3], Pronaya Bhattacharya[4], and Sudeep Tanwar[1]

[1]Nirma University Institute of Technology
[2]National Institute of Technology Patna
[3]Sardar Vallabhbhai National Institute of Technology
[4]Nirma University

January 30, 2024

Abstract

Recently, blockchain-based IoT solutions have been proposed that address trust limitation by maintaining data consistency, immutability, and chronology in IoT environments. However, IoT ecosystems are resource-constrained and have low bandwidth and finite computing power of sensor nodes. Thus, the inclusion of blockchain requires an effective policy design regarding consensus and smart contract environments in heterogeneous IoT applications. Recent studies have presented blockchain as a potential solution in IoT, but an effective view of consensus and smart contract design to meet the end application requirements is an open problem. Motivated by the same, the survey presents the integration of suitable low-powered consensus protocols and smart contract design to assess and validate the blockchain-IoT ecosystems. We discuss the key blockchain concepts and present the scalability and performance issues of consensus protocols to support IoT. Further, we discuss smart contract vulnerabilities and blockchain attacks. Open issues and future directions are presented, supported through a case study of low-powered consensus protocol design in the blockchain- IoT ecosystem. The survey intends to drive novel solutions for future consensus and safe, smart contract designs to support applicative IoT ecosyst

Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

ARTICLE TYPE

A Transformative Shift Towards Blockchain-based IoT Environments: Consensus, Smart Contracts, and Future Directions

Chandan Trivedi[1,2] | Udai Pratap Rao[3] | Keyur Parmar[2] | Pronaya Bhattacharya[1] | Sudeep Tanwar*[1]

[1]Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India (chandan.trivedi@nirmauni.ac.in, pronoya.bhattacharya@nirmauni.ac.in, sudeep.tanwar@nirmauni.ac.in)

[2]Department of Computer Science and Engineering, Sardar Vallabhbhai National Institute of Technology, Surat, Gujarat, India (d19co001@coed.svnit.ac.in, keyur@coed.svnit.ac.in)

[3]Department of Computer Science and Engineering, National Institute of Technology, Patna, India (udai.cs@nitp.ac.in)

Correspondence
*Sudeep Tanwar, Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India (Email: sudeep.tanwar@nirmauni.ac.in)

Summary

Recently, Internet-of-Things (IoT) based applications have shifted from centralized infrastructures to decentralized ecosystems, owing to user data's security and privacy limitations. The shift has opened new doors for intruders to launch distributed attacks in diverse IoT scenarios that jeopardize the application environments. Moreover, as heterogeneous and autonomous networks communicate, the attacks intensify, which justifies the requirement of trust as a key policy. Recently, blockchain-based IoT solutions have been proposed that address trust limitation by maintaining data consistency, immutability, and chronology in IoT environments. However, IoT ecosystems are resource-constrained and have low bandwidth and finite computing power of sensor nodes. Thus, the inclusion of blockchain requires an effective policy design regarding consensus and smart contract environments in heterogeneous IoT applications. Recent studies have presented blockchain as a potential solution in IoT, but an effective view of consensus and smart contract design to meet the end application requirements is an open problem. Motivated by the same, the survey presents the integration of suitable low-powered consensus protocols and smart contract design to assess and validate the blockchain-IoT ecosystems. We discuss the key blockchain concepts and present the scalability and performance issues of consensus protocols to support IoT. Further, we discuss smart contract vulnerabilities and blockchain attacks. Open issues and future directions are presented, supported through a case study of low-powered consensus protocol design in the blockchain-IoT ecosystem. The survey intends to drive novel solutions for future consensus and safe, smart contract designs to support applicative IoT ecosystems.

KEYWORDS:
Blockchain, Internet of Things, Security, Privacy, Consensus, Smart Contracts, Healthcare

1 | INTRODUCTION

With the constant upgrading of sensor-enabled terminal devices and the development of new communications network technologies, the services based on the Internet of Things (IoT) are growing these days exponentially[1,2]. It is envisioned that by the end of 2025, the number of IoT devices may reach 20-25 billion[3]. A large number of terminal connections and services

enable people towards great convenience with applications, such as smart buildings, remote monitoring, smart homes, smart cities, intelligent transportation systems (ITS), smart healthcare, and smart drones[3,4,5]. IoT provides services to end-users by enabling physical devices as components. Nodes in this environment need communication interfaces and identified via some unique address (i.e., identifier) over the Internet[6]. These nodes can be classified into different categories, such as the service node, intermediary node, and physical node.

In recent years, various architectures based on the layered concept proposed by eminent researchers are mostly referred to

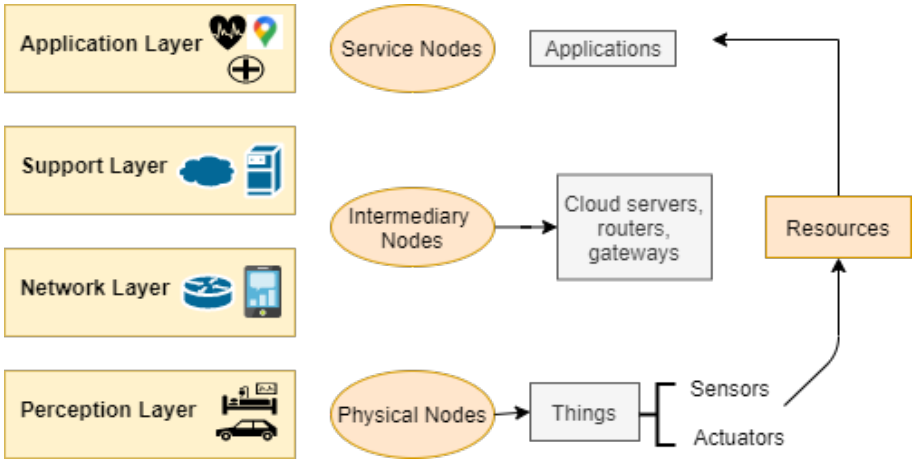

FIGURE 1 Four layer architecture with nodes in IoT Environment

as three-layer[1], four-layer[7], and five-layer models[8]. Our paper considers the base of four-layer architecture. We consider an IoT architecture that correctly handles network functionalities and requirements. **FIGURE** 1 displays the overview of nodes and their presence in a layered architecture. As IoT progress with many advancements in protocols and architectures that satisfy the basic requirements of applications, we try to summarize the functionalities of four-layer architecture for IoT based on standard TCP/IP layered model in **TABLE** 1.

With modern wireless communication support of 5G and beyond networks[9], IoT and blockchain will play a significant

TABLE 1 Layers and functionalities in IoT Environment

Layers	**Functionalities in IoT**
Application	Logic, data semantics, data presentation, Smart APIs, Data access management, service delivery
Support/ Cloud	Storage, computation and decision making, processing of data, Interoperability, and connectivity (Ex. Cloud Platform)
Network	Networking, data transfer to Cloud and information of protocols
Perception/ Sensor	Sensing, actuating, resource production, power supplies, and control capabilities

role in real-time decision-making using fog computing[10], edge computing[11], and many others. Thus, it becomes essential to understand the basic security standards during the development of IoT applications. The IoT environment deals with physical objects like wearable devices and sensing devices that capture personal data and monitor sensitive data. These data reside in an open environment that can lead to alteration, unauthorized access, and information misuse by malicious nodes and breach users' security and privacy. So, IoT's primary objective is to provide suitable authentication methods, confidentiality, integrity, and availability of data[12,13]. However, the key process of handling security includes authentication techniques, access control

methods, trust management, policy management, and secure protocol configuration [14]. Here, authentication refers to verifying a user's or device's identity while access control rules defining rights and protection assigned to the user within the IoT network. The primary goal of access control is to restrict authenticated users' privileges to guarantee the defence against malicious access to the resources.

IoT is a widely used trend in the technology field with applications running on heterogeneous devices that may have different topology for communications depending upon the adapted architecture style [2,10]. Moreover, architecture can be centralized or decentralized. Centralized architecture depends on network layer devices such as routers that forward information to applications and support layer services, i.e., the cloud as a resource provider to fulfill users' computation and processing needs. If the support layer (i.e., cloud services) fails to do so, it leads to the entire communication failure [15,16]. Currently deployed centralized architectures that overcome privacy and security are based on high-processing servers owned by third-party organizations where end-users need to trust them for handling their private data [17,11]. These data may be misused and shared by the trusted third party (TTP) to other parties for their benefits. Following are the challenges in the centralized IoT architecture

- If centralized servers fail, the entire network may go down. There is also the possibility of Denial-of-Service (DoS) attacks [6] that can result in a single-point failure problem in the IoT networks [14].
- In an application like smart healthcare, patient records become crucial information. In this case, using a centralized server may misuse the records and cause a loss of control over their data. So, there is an issue of accountability and traceability of records with the threat of data tampering [18].
- The exponential growth of IoT leads to insufficient communication processing in a centralized way. So, scalability becomes an issue in this case. [19,20].

Considering the above challenges in the IoT ecosystem, a decentralized architecture was introduced that enables direct communication between physical nodes when there is no need for support layer services [21]. Decentralized architecture provides additional fault tolerance and minimum delay feature between end devices [17]. So, for heterogeneous devices, the diversified, and resource-constrained environment, it enhances the quality and response time [3,19]. It doesn't wait for a decision from computing servers in the support layer. Decentralization also enables peer-to-peer communications that help resource-constrained IoT devices by fast computation without TTP in the support layer. When we think of adopting the decentralized approach, blockchain technology is trending and evolving with an immutable ledger, security, and distributed infrastructure as key features. These features of blockchain can be used in IoT to provide solutions to the challenges mentioned in a centralized architecture.

FIGURE 2 shows the global market to contribute to blockchain IoT envisioned industry. Discussion in Banerji et al. [19] and

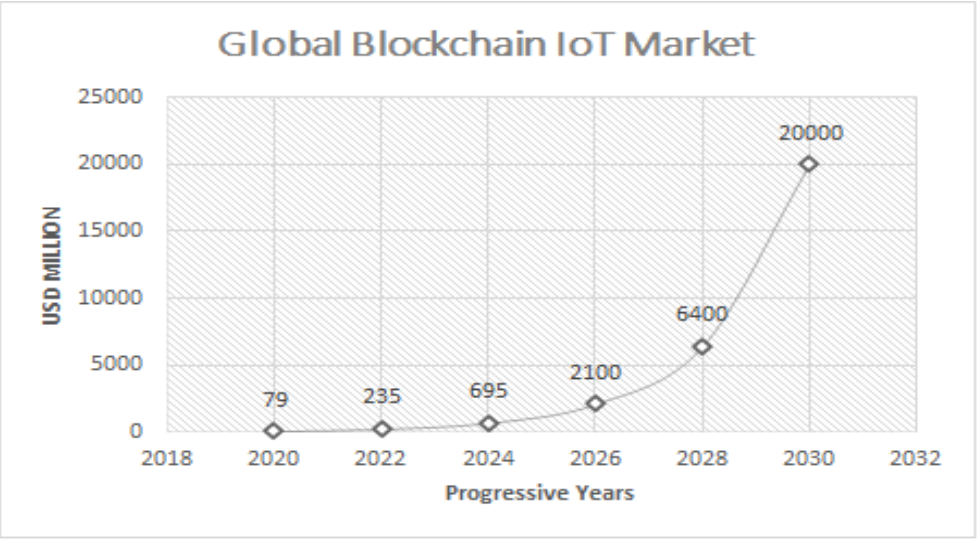

FIGURE 2 Global blockchain IoT Expected Growth

Roy et al.[22] show that using blockchain seems to be prominent for providing strong security and privacy in a resource-constrained environment. The blockchain became popular from the concept of bitcoin cryptocurrency originally proposed by Nakamoto[23]. Bitcoin uses distributed ledger to run transactions in a self-managing network. Later, these concepts become a part of the finance industry, logistics, and supply chain industry and now evolving to its integration with IoT[24,25].

Blockchain enables a trustful environment using cryptographic security and without central servers, so data reconciliation becomes faster. Other properties such as distributed ledger and immutability make it server-less; thus, record-keeping and data maintenance achieves consistency and transparency[26]. Using blockchain for decentralization in IoT has become famous for researchers as it gives the following advantages.

- Blockchain solves the issue of fault tolerance and single-point failure in a centralized infrastructure. Also, it removes the dependency[27] on TTP such that the privacy of critical records are maintained.
- It focuses on peer-to-peer communication and automation based on the smart contract, thus eliminating the processing of data[19] through a centralized server.
- Blockchain allows verifying participants and user identities based on consensus mechanisms and public key infrastructure[28], leading to better privacy and strong security in the network.
- Logs in the system become immutable, which leads to the assurance of traceability and accountability[29]. While smart contracts on blockchain platforms are capable of self-executing transactions,[30] based on communication logs, thus enhancing the functionalities such as authentication and access control that ensures security in IoT[31,27].

During the evaluation of the IoT areas, researchers have their grouping of regions and applications. Each scientific categorization or application has its benefits, depending upon the target to be accomplished and the definition and setting of the IoT constraints. IoT-based smart applications with integrated blockchain features may overcome fault tolerance, security, and privacy limitations[32]. So, We have summarized the advantages, key benefits, and weaknesses of trending IoT applications in our study using **TABLE** 2.

Moreover, **TABLE** 3 presents a summary that helps us identify the key research area for decentralization while preserving IoT's

TABLE 2 Use Cases, Advantages and Threats in Various IoT Applications

Applications	Attributes and Use cases	Advantages	Threats
Smart Transportation[2,33]	Automatic and efficient traffic control, Remote connectivity, toll, and transport data (RFID) maintenance, Vehicle tracking	Effective management of traffic, Fewer accidents, Fast toll tax payment	Delay in communication result may have a considerable loss, RFID security
Smart agriculture[8,24]	The remote stock calculation, Moisture sensing in soil, Weather analysis, shipping of agro-products, track records	Remote farming, Water waste management, Handling environmental conditions	Delay in status, lack of attention, Economic loss
Smart homes[27,29]	Remote control, Adaptable home environment, a customized physical task, water management	Time-saving, Convenience, Customization	Interdependence, High volume, Heterogeneous device handling
Smart grid[2,34]	Tracking resources for electricity suppliers, automation, tariff records, Pattern analysis of power usage	Cost effective, Reliable, Electricity charges reduction	Fault tolerance, monetary loss in case of cyberattacks, Interoperability
Smart healthcare[3,28]	Connected healthcare services, Smart bio-sensors for monitoring patients, EHR records tracking	Access from anywhere and availability, Early detection, and prevention of diseases	Patient consent, data theft, malicious code injection in bio-sensors
Smart industry[1,18]	NFC and RFID tags, maintenance based on prediction, product data tracking, production and packaging data, delivery transactions data	Efficient resource management, Cost effective	Distributed storage and computation
Smart city[7,35]	Efficient water distribution, Waste management, Environment monitoring, Urban Security, Pollution control records, Smart properties	Reduction in noise and pollution, Less wastage of water, Safe cities	A constraint sensor node, Side-channel analysis, DDoS, Tempering data, Privacy of citizens

TABLE 3 IoT Features with Threats, Challenges, and Solutions[2,6]

Feature	Key aspects	Threats	Challenges	Solutions
Closeness (touch)	Direct contact with the human body for observation Ex: wearable devices	User Privacy, without consent sharing	Privacy protection, access control	Data masking, encryption but it may introduce delay and lack of originality
Diversity	Heterogeneous devices, Ex: smart city	Security breach in protocols, insufficient device authentication, Resource allocation	Common security architecture	Dynamic analysis for embedded systems, Linux based only
Multitude (large scale)	Huge amount of data and a large number of devices, scalability Ex. smart grid, smart city	Distributed denial of services (DDoS), botnets in IoT	Stop the spread of botnets and IDS	Prevention Methods are specific to protocols and applications
Constrained (limited)	Small and lightweight, real-time processing, power consumption Ex. Smart grid, smart home	Memory safety integration, Denial of service, computation prediction, side-channel analysis	Lightweight encryption, embedded computing resources, scalability or optimization	Biological features, side-channel and PUF.
Flexible	Mobility, Heterogeneous environment, frequent movement, communication to unknown devices Ex. Smart transportation	Injection of malicious code and changing configuration	Cross-domain identification and trust management, permissions in the mobile environment, data confidentiality, and protection	dynamic security configuration but not in-depth
Unattended (long run)	Use for long period without physical access, Ex. Smart meter, agriculture, etc.	Infect program logic by a remote attack that leads to bodily damage	Remote verification of device status	Delay introduced in existing techniques, Lightweight but no handling of exception
Mutuality	Dependency on implicit controls, Interdependence in devices, Ex. Home automation	Bypassing security mechanism and over privilege	Physical security, Access control Privilege management	Context IoT user decision-based only
Omnipresent (Ubiquitous)	Rely on IoT devices in daily life	Design flaws by manufacturers, insecure configuration	Awareness to operators, manufacturers, and consumers	-

essential properties for integrating blockchain concepts. This will open up issues like anonymity, active device participation, authorization mechanisms, scalability, privacy, and many more in the current IoT environment. Further, these key features should not be ignored while adopting blockchain concepts in IoT.

1.1 | Motivation and Necessity of Survey

Many researchers worldwide have become more focused on the blockchain to resolve IoT's trust, privacy, and security concerns due to its underlying cryptographic security benefits and properties. Blockchain concentrates on decentralization, pseudonymous identities, fault tolerance, authentication, transaction integrity, and immutability. However, integrating blockchain in IoT can lead to problems in latency in transactions, scalability, smart contract vulnerabilities, intensive computation, energy requirements, ample storage, and privacy flaws, so the suitability regarding consensus and designing smart contracts must be considered. Thus, blockchain's features motivate us to see its integration with the IoT Ecosystem and analyze issues and challenges in this new paradigm shift.

1.2 | Our Contributions:

- We have identified issues and requirements of IoT towards decentralization with the integration of blockchain properties
- We have presented insights on the use of smart contracts, consensus, and their applicability in resource-constrained IoT networks.
- Our work compares various consensus, implementation platforms, and security parameters for providing future direction and current progress of blockchain and IoT integration
- We identified challenges and possible research direction by forming questions that researchers can address in the future.
- We have presented a case study on smart healthcare and the integration of IoT and blockchain concepts for medical devices.

1.3 | Article Structure

In section 2, we present a background study and related work to reach details of IoT-blockchain integration aspects. In section 3, we summarize related issues and challenges currently present in the blockchain-based IoT incorporating consensus and smart contracts in detail. Section 4 offers analysis and significant areas that need improvement during blockchain integration in the

IoT environment. In section 5, we present a case study using blockchain in healthcare. At last, section 6 leads to a conclusion of the study.

2 | BACKGROUND STUDY

This section presents the basics of blockchain and related work to integrating IoT and blockchain.

2.1 | Requirements in Blockchain-enabled IoT

Blockchain fulfills certain conditions and requirements of IoT and makes it more suitable for many smart applications mentioned in **TABLE** 3. We have identified some of the major requirements and classified concerning security and performance, as presented in **FIGURE** 3. These requirements will be used to analyze the decentralization level based on the significance of various parameters in IoT-blockchain collaboration[28,36].

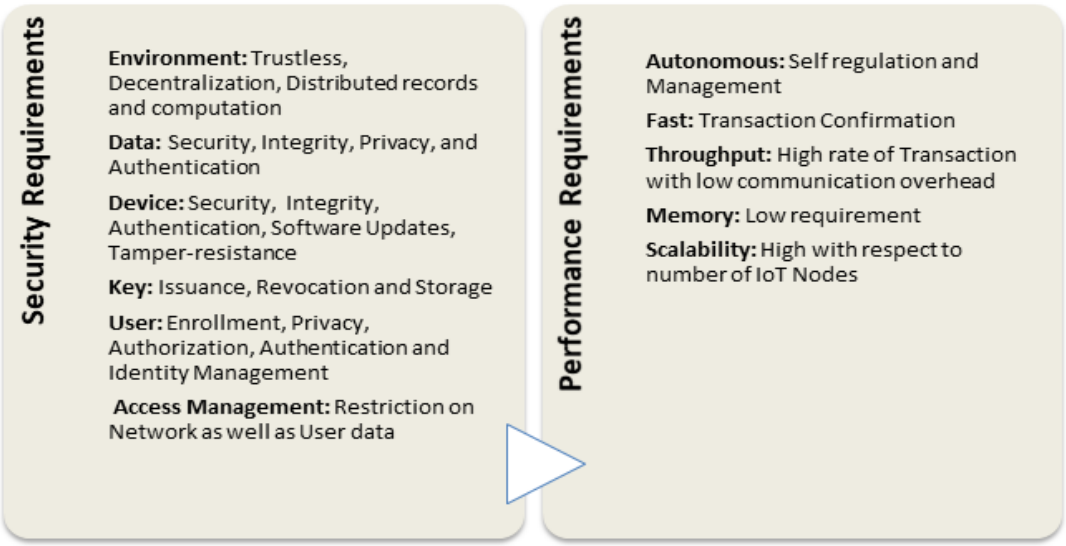

FIGURE 3 Classification of IoT Requirements for blockchain Integration[14,36,33]

2.2 | Blockchain

Blockchain is a distributed, digital ledger based on cryptographic properties that perform the append-only operation in public accounting without TTP. Blockchain can complete transactions trust-free, where every action request has a record on the chain with a digital signature for public verification[24]. Participants in the systems are responsible for creating and maintaining the ledger. Blockchain uses the underlying principle of public key infrastructure and an economy-based model for networking and providing consensus to achieve consistency, transparency, and coordination in distributed databases. With digital currencies, the ledger is the key application to keep records, and it could potentially be adapted in networks where a primary requirement is data sharing, fault tolerance, and record tracking[18]. For analyzing, the applicability of blockchain in the IoT ecosystem, it is essential to understand features, working principles, and underlying concepts.

2.2.1 | Key Concepts

Blockchain is a ledger with distributed networking comprised of serial linking transaction blocks or logs within the network. Transactions are considered an operation resulting in the change of state in the blockchain. A transaction varies from financial

asset transfer to the execution of arbitrary code in the form of a smart contract, depending on the network. In the case of an IoT ecosystem, a transaction can be a way to exchange data from users or vice-versa [11,22]. Block is a collection of all transactions that have occurred in the past and are not verified yet. It further splits into two parts, a block body and body, where the header maintains a timestamp, hash of the previous block, Merkle root hash of all transactions, and a random number nonce [23,15]. **FIGURE** 4 shows the elements and structure of a block.

A block uses the private key as signing transactions and the public key as verification of transactions in a distributed ledger-based public network. A Merkle root contains a tree of hash usually employed to generate a hash value of all the transactions in the current block to minimize the chain's storage overhead. A header consists of a hash from the previous block, which is used to create a hash of the current block and stores a hash that links the next block, thus making the ledger tamper-proof. Further, block broadcasting happens in the network after collecting all transactions, and then some miners validate all transactions in that block [37,38].

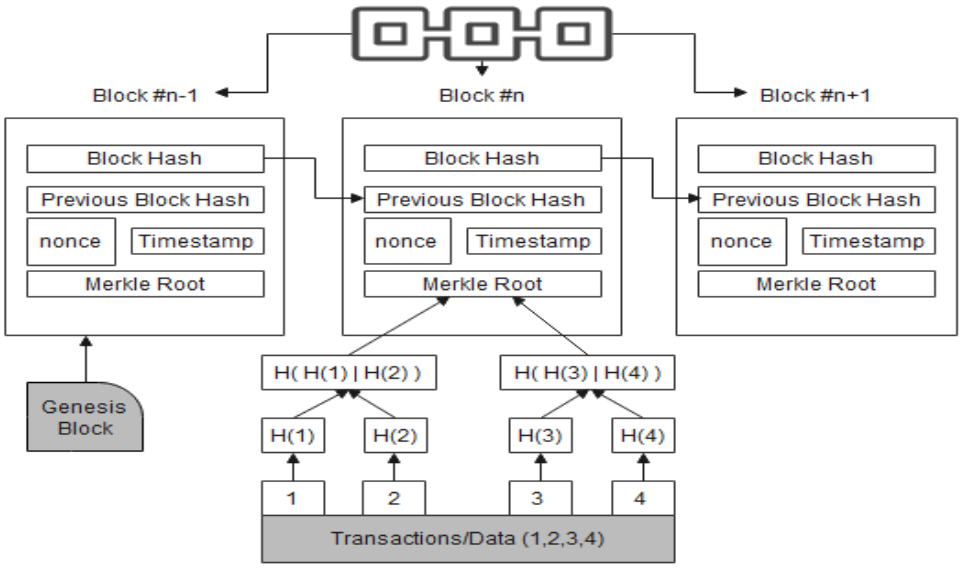

FIGURE 4 Structure of Blockchain

Mining refers to adding validated transactions to a block and then broadcasting that block on the blockchain network to inform all other nodes about its current status. Miner nodes do the mining. A node's selection to mine a new block is based on specific lottery schemes, depending on their capacities and resources, such as computational capacity and memory space [17]. The blockchain nodes are categorized into three ways. A Simple Node sends and receives a transaction and does not store the complete copy of the blockchain. In the IoT environment, a simple node can be a sensor node that can only send readings to a gateway device or going to receive some instructions in return [2,39]. Other than that, full Nodes are not participants in mining but maintain the complete copy of the blockchain and use consensus-based validation rules with the feature of block propagation. Full nodes are essential for security purposes in IoT because double spending can not route through these nodes [12,40]. Lastly, Validator or Miner Nodes are full nodes capable of mining and validating blocks. These nodes are selected based on consensus mechanisms like PoW [23], where the miner must solve the cryptographic hash puzzle, and the node who answers it first will become a miner. In the case of bitcoin, the miner node must apply a PoW consensus so that the rest of the participants can verify the puzzle and identify whether it is resolved. If the rest of the participants approve the network block, then the miner node is awarded in some cryptocurrency.

2.2.2 | Properties of Blockchain

In this section, we discuss the properties of blockchain, such as decentralization, independence, anonymity, transparency, etc.

- **Decentralization:** Blockchain is a decentralized public ledger where data is stored across its peers in the network. In blockchain, there is no central entity or authority to store data; thus, it is not vulnerable to a single point of failure. Moreover, there is no need for a third party due to decentralization[33]. This feature can help to resolve scalability issues in the IoT ecosystem.

- **Independence:** No one can govern the blockchain while collecting, transferring, and updating the ledger based on consensus. Consistency is assured by agreement and achieves accuracy without needing any trustworthy third party[41,34].

- **Anonymity:** Tracing an actual account user's identity in the blockchain network is technically impossible. The identity is hidden behind cryptographic primitives like a digital signature for authenticating users and monitoring their access[42]. Constantly changing private keys is facilitated to sign each transaction digitally for IoT users' actions. Hence, anonymity is ensured through source authentication and identification[34].

- **Collective verification:** A specific transaction is added to the blockchain model only after other participating nodes verify and validate it. So, Collective identification and verification remove the need for a third party in blockchain applications, so a single party handles "no computation"[14].

- **Transparency:** In the blockchain, every entry and update requires authentication and validation by the system. Hence, fraud transactions are minimal, making any changes in a distributed ledger impossible. So, this leads to a higher level of transparency in the blockchain system[25,26].

- **Security:** A hash tree-based Merkle tree in block enables security as its chaining makes it tamper-proof. Nodes utilize a consensus mechanism in the network to validate a block, and each block's digital signature provides strong blockchain security in blockchain[22]. It uses the public key cryptography concept, i.e., digital signature for transactions in each block. So if any information alteration occurs, the digital signature denies the same. From a decentralization perspective, all data are broadcasted in a network, and peers maintain an immutable copy of the broadcasting information[43]; thus, it requires enormous computing power to modify any information from a single point in the blockchain.

2.2.3 | Categories of Blockchain

We briefly discuss the categories of blockchain, considering its properties in this subsection.

- **Permissionless Vs. Permissioned:** Blockchain is categorized into two parts: permission, permission, and permissionless based on new block generation, transaction processing, and validation[44]. In permission, blockchain allows only selected nodes to participate that generate and validate a transaction block. In a permissionless blockchain, any node can validate and create transactions or blocks[28].

- **Private, Public, and Consortium Blockchain:** Blockchain types are defined based on their access rights in the system. The system where nodes, participants, and validators who want to contribute to the blockchain need to take permission from the authority of an organization referred to as a private blockchain. Whereas the Public blockchain doesn't restrict nodes from joining the network, i.e., anyone can send or receive information and participate in the consensus mechanism. Ethereum[45] and bitcoin[23] are the two public blockchain platforms, while hyperledger[46] provides a private blockchain environment. Another blockchain known as consortium blockchain is considered partially decentralized, where a group of organizations monitors nodes for processing the information[36].

2.3 | Related Work

As blockchain is an emerging technology, many researchers are trying to see how to integrate it with IoT. Therefore, we identified papers published related to the integration and survey that provide details on the parameter such as security, privacy, consensus, smart contract, and integration in **TABLE** 4.

In a survey of Conoscenti et al.[24], discussion on blockchain adoption in IoT is a key focus with the property of anonymity. They have yet to consider consensus adoption for lightweight IoT integration in this work. However, Yeow et al.[47] discuss the edge-centric consensus and its applicability in IoT. They have partially introduced how smart contracts are beneficial in this paradigm shift. In the work of Roy et al.[22], they provide insights into the blockchain structure and its applicability in IoT and also discuss the challenges in adopting it for the management of IoT devices. Moreover, the consensus for IoT devices and their privacy needs

TABLE 4 Related Work for Integrating Blockchain and IoT

Paper	Year	Parameters considering IoT and Blockchain					Key Contributions
		Security	Privacy	Smart Contract	Integration	Consensus	
[24]	2016	Yes	Yes	No	Partially	No	Discussion about anonymity, use cases and integration benefits
[47]	2017	Yes	No	No	Yes	Partially	Discuss the edge-centric consensus and its applicability in IoT
[48]	2017	Yes	Yes	No	No	No	Discuss the details of security and privacy parameters with emerging issues in IoT
[22]	2018	Yes	No	Partially	Yes	No	Provides insights into the blockchain structure and its applicability in IoT, also, discuss the challenges in adopting for management of IoT devices
[1]	2018	Yes	Partially	Partially	Yes	Partially	Details of IoT features and their challenges, discussion about adopting blockchain-based solution and future opportunities
[28]	2018	Yes	No	Partially	Yes	Partially	Discussion about performance and platforms in IoT blockchain integration, also presents challenges, analyses and, features
[36]	2019	Yes	Yes	Partially	Yes	No	Discussion is towards integration aspects and the parameters with implementation requirements and open issues. Focus on Cryptocurrency and decentralized storage
[37]	2019	Yes	Yes	No	Yes	Partially	Discussion towards the integration advantages and PoW and PoS consensus and, also presents comparative performance
[49]	2019	Yes	No	No	Yes	Partially	Survey on existing approaches with applications, consensus, and opportunities, discussion on the performance of PoW, PoS, and Byzantine consensus and its applicability
[14]	2020	Yes	No	No	Partially	Partially	Survey and comparative study of blockchain integration for Industrial IoT and Attacks and Security issues are discussed in detail.
[50]	2020	Partially	Partially	No	Yes	Yes	Focus is more towards consensus and IoT adoption, research challenges and opportunities discussed with performance and requirements in resource constrained IoT area
[51]	2020	Partially	Partially	No	Yes	Yes	Survey on consensus specific to performance comparison of PoW, PoS and pure-PoS
[52]	2021	Yes	Yes	Partially	Yes	Partially	Presents a survey on the feature of blockchain, security issues, challenges and solution for IoT domain, impact and use cases discussed
[53]	2021	Yes	No	No	Yes	Partially	Presents survey on application based integration for cloud IoT and fog computing
[54]	2022	Yes	Yes	Partially	Yes	Partially	Presents insights to applications and its integration scenario to blockchain but limited discussion on consensus and smart contract
[55]	2022	Yes	Partially	Yes	Yes	No	This paper discuss about security concerns and their solutions for next generation IoT integration
Our Paper	-	Yes	Yes	Yes	Yes	Yes	Discuss the applicability of smart contract, and state challenges and attacks during integration, Insights to consensus and platforms for decentralization and provide sub-area, Future directions under the integration of blockchain and IoT

to be improved in their integration architecture. Khan et al.[1] include IoT features and their challenges with the discussion of adopting blockchain-based solutions and future opportunities. A brief idea about the suitability of consensus and smart contracts gives an overview of the integration scenario in a general sense. In Moin et al.[36], they are inclined towards integration aspects and the parameters with implementation requirements and open issues. The focus is more on Cryptocurrency and decentralized storage The survey contribution of Wang et al.[49] discuss existing approaches with applications, consensus, and opportunities. They consider the performance of PoW, PoS, and Byzantine consensus and its applicability to the IoT environment. Next, Salimitari et al.[50] cover the details of consensus protocol and its suitability without considering the impact of those consensuses on lightweight IoT devices. Still, their work provides a complete view of basic consensus implementation. Moreover, Lepore et al.[51] discuss the performance of basic consensus methods and their comparative study in detail. The new pure-PoS consensus is also considered in their work. In Xu et al.[52], the survey on the feature of blockchain, security issues, challenges, and solutions for the IoT domain with its impact and use cases were discussed. Some of the articles discuss more on integration challenges without considering broad areas of applications and all the features. For example, another survey by Uddin et al.[53] presents application-based integration for cloud IoT and fog computing. Moreover, they have specifically discussed the cloud-based blockchain properties without smart contract deployment. Recently Abdelmaboud et al.[54] gave insights into applications and their integration scenario to blockchain but limited discussion on consensus and smart contracts. Moreover, Tanwar et al.[55] have developed detailed taxonomy and next-generation IoT and blockchain integration. Li et al.[56] proposed new insights on service models on blockchain, named as Blockchain-as-a-Service for cloud providers. The article categorizes the recent studies on the applied scenarios.

In contrast, some of the surveys discuss only consensus or only security and privacy issues. Many authors have tried to emphasize specific consensus and performance while some partially addressed the concept of smart contracts, issues, and challenges its applicability towards resource constraint devices.

By state of the art, we concluded to provide insights on more consensus concerning IoT. Also, we tried to discuss the approach with one of the subsections with the smart contract and its details in integration, which differentiate our work from others. We also present the various platform and formed future opportunities using a question-based approach. This approach offers a better understanding of future research questions and covers multiple areas where the IoT needs blockchain-based extension and improvement.

3 | NUTS AND BOLTS OF BLOCKCHAIN AND IOT INTEGRATION

Blockchain and IoT are new technologies that'll be integral in future networks. Both the technology have integration of both can achieve efficient and secure systems. This section reviewed the related work of various consensus mechanisms and smart contracts. Further, we inferred some issues and challenges in integration and presented a comparative study. Additionally, **FIGURE** 5 presents the possible benefits of Blockchain-IoT integration, different design strategies, conceptual views, and its principle.

3.1 | Consensus Mechanisms

The consensus design is based on liveness, fault tolerance, and safety. Liveness means having uninterruptible and smooth working of distributed process runs for all correct nodes in the fault tolerance system even if f faulty nodes are present[11,41]. In a fault-tolerant system, $S(N, f)$ safety is defined as the failure of nodes it can resist, where the number of faulty nodes is f, and a total number of nodes are n. Safety is the capacity to mitigate corrupted or out-of-order messages so that every node functioning correctly can agree on valid outcomes to the state machine's rules. Consensus mechanisms have been an active research area since the very introduction of the blockchain. It is a crucial component of any blockchain network that allows for the distributed operation of its system by requiring consent from all participating nodes before a new block is added. Security and robustness in blockchain networks enabled by consensus mechanisms[50]. Consensus mechanisms seek to update replicated states safely and run as a critical piece of the blockchain's working principles puzzle. The blockchain's state machine replication consensus mechanism ensures that all copies of the same state are synced and accepted at all times. Fully asynchronous communication models may not be fault-tolerant, which becomes a critical issue in the system, so we need to assume partial synchronous communication with maximum thresholds for latency of propagating transactions[17]. A well-known Proof of Work (PoW) mechanism is used in bitcoin[40]. In comparison, other mechanisms such as proof of stake(PoS), extended PoS[41], class

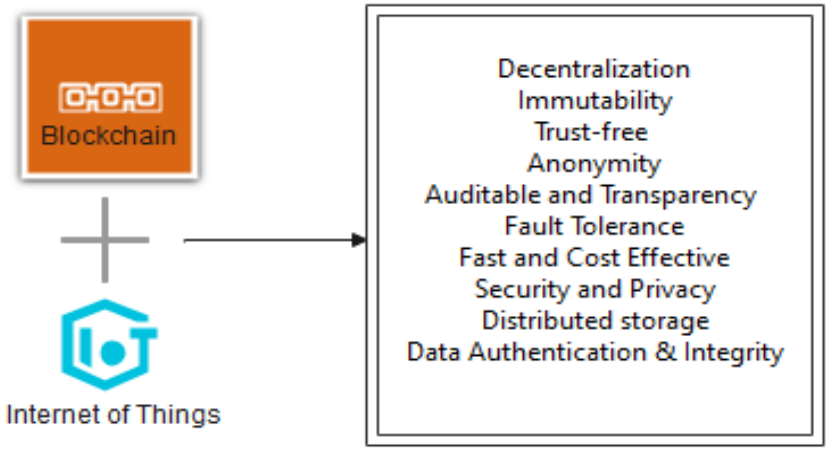

FIGURE 5 Benefits of Blockchain with IoT

of byzantine fault tolerance(BFT), algorand, ripple, stellar, and IOTA were introduced later to overcome limitations like fault tolerance capability, less computation, faster execution, maximum throughput, and broad applicability[47,19]. In papers[19-50], some partial synchronous and digital currency prototype designs and ideas are presented that make foundations for creating "decentralized" consensus mechanisms used in blockchain networks. We studied earlier mentioned decentralized consensus[37,50] used in blockchain, and summarizes various working principles and applicability for resource-constrained IoT networks based on affecting parameters.

- **Proof of Work (PoW):** It is a computationally expensive mechanism that includes enormous processing power to solve the puzzle for proposing blocks during mining by miners. This method used the SHA-256 algorithm and produced 256-bit output with the hash value[57]. The proposed block by some miners consists of nonce, hash of the previous block, and timestamp. Finding the nonce value by the miner releases the next block to other nodes. Other participants can verify the same and claim the perceived nonce value that becomes an input to the SHA-256 function for hash generation, and other miners can withdraw their power and go for the next block mining. If the output is less than the target hash, then the nonce will be discarded, and others do start mining by proposing some new nonce. This mechanism's mathematical process of finding hash is very time-consuming and can be solved using the brute-force technique. Bitcoin uses PoW[23] that takes 10 minutes to mine a block as per a defined hard mathematical hash-based puzzle. However, due to its incentive-based and computational expensiveness, it resists DDoS, and network attacks[58]. Suppose the attacker compromises more than $1/2$ of total computation power. In that case, it becomes vulnerable so that it can tolerate fault up to $2f+1$. Here, f represents faulty nodes that occupy processing power. Yet another possibility of generating a fork in the system may result in late consensus finality. PoW was the best-suited cryptocurrency introduced as bitcoin, and because of the computationally expensive procedure, it is vulnerable to public network regarding and has a threat of Sybil attack. But its higher bandwidth and computational power put limits on uses in the resource-constrained IoT environment[37].

- **Proof of Stake (PoS):** This mechanism eliminates the computation of expensive puzzles in PoW. It provides an alternative to utilize participants' stake based on their economic share and age in-network, while the rest procedure is the same as PoW[51]. This mechanism introduces attacks like "nothing in share" and monopoly having more than $1/2$ of total stake coins all time due to stakeholders' higher economic status or maybe gaining stake continuously because of the coin reset concept. Block finality is improved in PoS compared to PoW because it doesn't use challenging mathematical computation. Additionally, the age of the coin has an inverse relationship with mining difficulty. So the different attacks mentioned in PoW are also possible and prone to forking in blockchain[27]. Some extended mechanisms, such as Delegated Proof of Stake (DPoS), work democratically[41]. All the stakeholders follow voting-based delegate selection and are responsible for mining the next block in blockchain. Here delegates are accountable for managing rewards, the size of a block, and transaction fees. This mechanism is capable of ruling out malicious delegates through voting. However, these mechanisms

show significant improvement toward IoT adoption based on their higher throughput and low latency, dependency on stakes limits their use in a constrained environment. Another version-extension-based proof of stake, i.e., leased PoS, leads towards adopting decentralization by enabling low-balance users to take leases from high-balance users based on the contracts[25]. Yet again, this LPoS is governed by the monetary concept, so not suitable for IoT. Proof of Importance (PoI) works on the principle of including reputation and digital currency for selecting the next miner in the system. Again, this mechanism suffers from IoT adoption because of monetization even after high throughput and low latency[37]. Casper is introduced based on PoS that works with GHOST protocol. It uses fork removal in blockchain and shows significant improvement in security and delay, But it can't be adopted in IoT because of digital currency involvement. Another proof of activity method (PoA) uses a mixture of PoS and PoW with a hash function-based header for group validation based on signing to reach consensus[50]. This mechanism has resistance against attacks, but it can't apply to delay-sensitive constrained IoT networks due to higher delay[17].

- **Proof of Burn (PoB):** This consensus utilizes the concept of spending digital coins on irretrievable addresses and burning coins in their accounts. Miners who have spent a significant amount of digital currency will be assigned priority, and they will get a chance to become miners for the next block in the system. However, IoT applications may not use currency-based transactions, and PoB practically offered digital currency. Thus, not suitable for resource-constrained IoT[19].

- **Proof-of-Elapsed Time (PoET):** This mechanism uses the concept of assigning miners for the next block mining based on their random waiting expiration first. Random waiting time solves miners' competence issues during PoW mining. PoET was initially proposed by Intel and can do mining based on its hardware, i.e., Software Guard Extension (SGX), having Trusted Execution Environment (TEE). This hardware verifies the correct expiry time to select the next miner based on winning random waiting[11]. This mechanism is computationally straightforward and suitable for IoT because of low energy consumption, low latency, and higher throughput. Simultaneously, blockchain's main property, i.e., decentralization, is violated because of Intel's hardware ownership.

- **Class of Byzantine Fault Tolerance (BFT):** This class of problems initially emerged from Byzantine General's issue. A scenario provides some general acts as malicious and tries to change the message, leading to inconsistency in loyal general decisions. Permissioned blockchains are more focused on this type of consensus because of the limited replicas needed to maintain and don't require costly proof to publish a block in the network. Blockchain is preserved from Sybil Attack[11,41].

- **Practical Byzantine Fault Tolerance (PBFT):** It is a critical consensus mechanism for asynchronous replica updates. It runs multiple rounds of voting for committing the current state of records and includes encryption and optimization to make it practical[33,43]. Solving the byzantine general problem requires $n >= 3f + 1$ nodes so that it can tolerate f faulty nodes. The following are steps to reach a consensus:

  1. In the first step, A leader will be selected to assemble all transactions to publish a block that will broadcast the network's original state.
  2. Now, Validator nodes will calculate the block's hash and start broadcasting it.
  3. Validating nodes get votes based on the hash values received from other nodes in the network
  4. If a candidate block gets 2/3 votes in his favour, it will be added the copy in the blockchain.

  High throughput and low latency parameters make PBFT consensus suitable for asynchronous updates. At the same time, broadcasting blocks and votes lead to overhead in a network[51]. Thus, scalability becomes an issue sometimes. Further, if this consensus used a Permissioned blockchain, it would become more suitable for small-scale applications like Smart Home.

- **Delegated Byzantine Fault Tolerance (DBFT):** Unlike PBFT, DBFT[36] requires the participation of limited nodes in consensus; thus, it becomes more scalable. It uses delegate selection that participates in agreement. Moreover, it is less suitable for IoT[59].

- **Algorand:** It combines pure PoS and BFT with Verifiable Random Functions (VRFs)[50]. A block in this consensus has VRFs based on unique member selection using the private-public key information. The disadvantage of these protocols is that they produce random seeds that may be biased towards the attacker, so the lock-back mechanism is used for unbiased seeds and strong synchrony[25].

- **Ripple:** Ripple makes use of Federate BFT and makes a unique-node list (UNL) for each server node that is responsible for consensus protocols[37]. On the other hand, client nodes are only used for transferring funds in the network. It reaches to consensus if $4/5$ of the total nodes agree. This protocol uses a monetary concept, but its high throughput, scalability, and low latency make it partially suitable for IoT[50,57].
- **Stellar Consensus Protocol (SCP):** This consensus mechanism operates on the working principle of federated BFT[47], a version of PBFT. Federated BFT uses an intersecting group to execute local consensus. SCP allows anyone to participate in the agreement. It uses quorum slices (i.e., a group of nodes participating in consensus) to achieve robustness. Ballot and nomination protocol is the base for running the consensus[57]. This consensus possesses high throughput and minimum computation, while latency is too low, making it partially suitable for resource-constrained networks.
- **Byzcoin:** It is BFT based mechanism working on the principle of collective signing, i.e., CoSi[60] to commit its state, thus making PBFT scalable. This protocol's tree structure has low latency but is vulnerable to Denial of Service attacks. In this method, PoW makes it less suitable for IoT, even with high throughput and scalability[17].
- **Tendermint:** A protocol that belongs to the BFT family, used primarily on permissioned blockchain. Unlike PBFT, each node in tender mint possesses different voting powers based on their stakes[61]. In this consensus, prevote and pre-commit stages are used for voting. The blockchain will add it when $> 2/3$ of validators run pre-commit for the same block in the same iteration. If monetary concepts can be replaced with other criteria, it becomes more suitable for IoT networks due to low latency, and high scalability[59,17].
- **IOTA:** It is a platform based on Tangle's[62] underlying concept that uses a directed acyclic graph (DAG) based structure and links two older transactions with each transaction[63]. So one transaction can approve more than two that can be added through PoW. Tip nodes are considered a new transaction in the system denoted using solid block squares, while approved transactions are indicated with white squares[1]. **FIGURE** 6 shows the structure of the tangle. It is a simple, infinitely scalable platform due to its unique tangle design, making it suitable for resource-constrained networks. Also, tangle does not have transaction fees which would be ideal for an IoT network. Contrary to different blockchain implementations, it is resistant to the phenomenon of quantum computing due to its particular structure design. Choosing approval for the two older transactions is the key issue with tangle and not enforcing any law. It's highly helpful for devices with limited resources in an IoT network to know how to choose these two nodes. The latest tangle implementation[63], IOTA, has only some of the proposed tangle objectives[64].

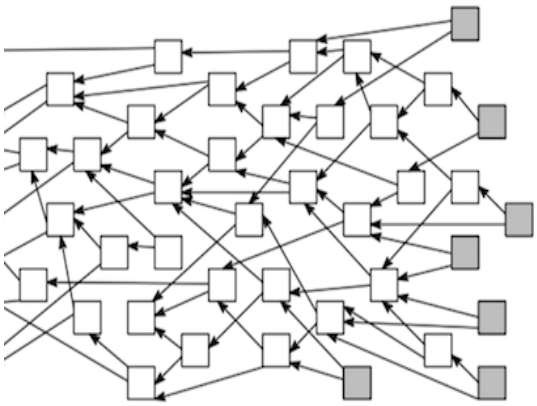

FIGURE 6 Structure of Tangle[62]

3.1.1 | Scalability and Performance Issues in Consensus Mechanisms

1. The overhead networking arising from voting processes limits allowable blockchains to just hundreds of nodes.

TABLE 5 Comparison between Various Consensus Mechanisms

Consensus	PoW	PoS	PoB	PoET	DBFT	PBFT	SCP	Byzcoin	Algorand	Tendermint	Ripple	Tangle
Category of Blockchain	PL	PL	PL	P, PL	P	P	PL	PL	PL	P	PL	PL
Type of blockchain	PU	PR, PU, CO	PU	PR	PR	PR, CO	PU	PU	PU	PR	PU	PU
Special Hardware	No	No	No	Intel SGX	No	No	No	No	No	No	No	No
Decentralize	H	H	H	M	M	M	H	H	H	M	H	M
Scalability	H	H	H	H	H	L	H	H	H	H	H	H
Throughput (TPS)	L	L	L	H	H	H	H	H	M	H	H	H
Latency	H	M	H	L	M	L	M	M	M	L	M	L
Adversary Tolerance	<25% CP	<51% CP	<25% CP	-	<33% Faulty	<33% Faulty	Variable	<33% Faulty	<33% Users	<33% Voting	<20% Faulty	<33% CP
Network Overhead	L	L	L	L	H	H	M	M	H	H	M	L
Computing Power	H	M	M	L	L	L	L	H	L	L	L	L
Storage Overhead	H	H	H	H	H	H	H	H	H	H	H	L

P - Permissioned, PL - Permissionless, H - High, M - Medium, L - Low, CP - Computing Power, PR - Private, PU - Public, SGX - Software Guard Extension, CO- Consortium, X - Unknown, BC - Blockchain, PoW - Proof of Work, PoS - Proof of State, PoB - Proof of Burn, PoET - Proof of Elapsed Time, DBFT - Delegated Byzantine Fault Tolerance, PBFT – Practical BFT, SCP - Stellar Consensus Protocol, TPS - Transactions per Seconds

2. The complexity for permissioned blockchain in worst case being $O(N^2)$ over $O(N)$ of permission blockchain[37]. It restricts the accessibility of permissioned IoT blockchain systems. So we can observe the trade-off between efficiency and performance concerning PoW and PBFT consensus[51,50].

3. Permissionless blockchains must have slower block genesis rates because of the propagation rates of network nodes. However, permissioned blockchains suffer from a major scalability issue despite having far reduced latency[36,49].

4. With the concepts of publicly accessible decentralization and transparency, Permissionless is more suited for industry-wide IoT implementation[34,65].

In **TABLE** 5, we compare several consensus mechanisms and discuss how well they work for the Internet of Things (IoT) applications in light of the relevant parameters used in various blockchain implementations. Also, blockchain-enabled IoT functionality and performance characteristics depend upon the underlying consensus method[66]. Any consensus approach, therefore, can only satisfy the expectations of particular applications. Therefore, specific criteria for implementing a functional blockchain-based network should be met according to the required framework. The most critical features for using a consensus mechanism when implementing a blockchain are a degree of decentralization, network reliability, protection, scalability, latency, overhead computation, networking overhead, efficiency, and overhead storage[67]. Many of those features become more critical concerning the desired application. Cryptocurrency is potentially the most attractive application for scholars in the blockchain field[24], and based on that; most of the consensus methods are considering cryptocurrency.[22,33]. With such a cryptocurrency, security and high throughput are essential. While low latency then becomes a critical issue. In a real-time IoT environment, a transaction can be submitted and completed very quickly[51]. However, the maximum of the existing consensus is lacking in latency and can meet resource constraint requirements partially. Even though low latency is essential for any of those IoT networks, more features are expected for better utilization.

However, other IoT networks, such the vehicular ad-hoc network (VANET), don't have a limited amount of resources and can function properly with a lot more overhead in terms of compute, communication, or area. Therefore, scalability does become a problem for smart transportation networks. Smart homes don't need to be very scalable, despite the fact that they are tiny networks of dozens of sensors and devices[27]. On the other hand, smart cities are made up of thousands of devices requiring high scalability[35]. Therefore, security and connectivity to networks are critical issues for Hybrid networks[68].

3.2 | Smart Contracts

Nick Szabo introduced the smart contract definition in 1997[69]. The smart contract (SC), compared to a conventional lawyer or notary, can act as a trusted third party without any speculation to help two parties exchange properties, land, securities, etc.[70]. However, these contracts are extended in programming logic and codes, which run automatically on the blockchain platform as soon as it satisfies the predefined conditions. Every party must finally achieve the results described in the system and get penalized as per the agreement[44]. Smart Contracts can execute themselves independently and automatically per the defined plan. Here parties involved in the transaction are the ones who can only agree but can't execute SC. So, alteration and corruption of data by a middle party are preserved, leading to autonomy[57,71].

In SCs, symmetric-key cryptography is integrated to secure documents on the distributed ledger. Hence, it is hard for a malicious user to tamper and infiltrate the codes, which can create trust issues. Besides these, SCs are cheaper, faster, and more reliable than traditional arrangements[15]. Smart contracts are executed on the blockchain platform and have a unique address referred to as DApps or decentralized applications. Invoking smart contracts requires an execution charge, as an invocation is considered a transaction recorded in the blockchain. Peers are encouraged to publish new blocks and thwart flooding attacks with execution rewards. SCs have clear visibility to all network participants, so security breaches can occur if participants encounter bugs, loopholes, or errors during execution. These security requirements need to address during smart contract design that runs electronic transactions and logs with various functionality and processing in the IoT networks[36,17]. Smart contracts can bring fast and secure handling in IoT applications like digital rights management, Auto-Pay, and Financial services like Insurance, Capital markets, Supply chain, Logistics, and Smart grid. Bitcoin posses minimal scripting capabilities, a current platform like hyperledger[46] and Ethereum[45] provides flexible support of smart contracts with Turing complete scripting languages. For Ethereum, solidity[45] and serpent[60] are trending languages to write smart contracts, while hyperledger uses Go[72] language, i.e., most suitable for permissioned blockchain.

3.2.1 | Issues and Challenges of Smart Contract

The centralized tradition of the Internet infrastructure is hard to fulfill IoT's technology needs, such as private data security and multi-device interaction trust. Instead, the variations, blockchain-integrated IoT, are becoming the latest trend. SCs can help simplify diverse workflows supporting the sharing of resources[2], saving costs, and ensuring security[59] and safety efficiency. Authors[35] discuss smart home implementation and explore various policy effectiveness in the model based on Blockchain and SCs. Their proposed model could reduce the daily rate compared to IoT devices controlled by simulation tests. Research in[15] coveres an architecture of smart contracts composed of multiple access control contracts, such as register and judge contracts to gain decentralized and reliable IoT system data access. The work of Zhang et al.[30] suggests decentralized privacy-based blockchain-IoT systems such as sharing economy, identity management, logistics, and supply chain.

3.2.2 | Smart Contract Vulnerabilities

- **Transaction-Command Dependency (TCD):** Every block includes different transactions and the order in which the execution of transactions relies upon the miner. Everything occurs when multiple dependent operations call in The same contract, which can be exploited by the miner for which the transactions are carried out[44].

- **Dependence Timestamp:** The miners can fix the value of the timestamp for the mined block (usually per the miner's regional clock system). Moreover, the miner can change the timestamp by a few seconds, assuming that other miners will support the proposed block. In this case, the weakness is that individual SCs take timestamps as a trigger condition, e.g., transferring money. Also, the opponent can exploit SCs by their interest, which is key loophole[3,28].

- **Performance Issues:** Blockchain performance concerns such as reduced scalability, bottleneck capacity, latency transactions, and storage constraints limiting smart contract efficiency, too. As an illustration of throughput, miners and validators perform SC in the new blockchain systems sequentially by miners and validators[34]. Here this concept of executing serial restricts device performance and fails to exploit the current multicore architecture with high clustering.

- **Vulnerability of Re-entrance:** A termination pending on the most recent execution when one contract calls another is a key aspect of re-entrance. As an attacker, the fallback mechanism in an intruder can use the call function to re-enter intermediate caller rank to execute regular calls that lead to invocation loops. In this case, the possibility of retrieving several refunds can make the balance empty.

3.3 | Various Attacks on Blockchain

As mentioned earlier, blockchain can achieve decentralization because of its properties but is vulnerable to security threats. We present some general attacks as follows.

- **Double Spending Attack:** The attack is aimed to puzzle the user with more than one identical transaction. An adversary launches a pre-mining attack on multiple blocks to create a conflicting transaction and fools the user into mining bitcoins for the same block [14].
- **Attacks on Consensus Mechanisms:** Consensus is an integral part of block validations, and thus, adversaries widely exploit attacks on consensus protocols. An adversarial system (with sufficient large computing and bandwidth capacity) attempts to reconstruct an alternating chain, where it forms a 51% majority consensus (as in the case of the PoW mechanism) [37]. For the attack to succeed, roughly more than 50% of the network hash power must be utilized by the adversarial node. To allow this, the adversary launches different schemes, which fools users into sharing their hash power with the node. If the adversary successfully solves the puzzle before anyone does, he becomes entitled to add the node to the alternate chain, which then becomes longer than the genuine chain. It would make the alternate chain genuine, and the attacker successfully takes the entire network control [73].
- **Eclipse Attacks:** Just as the name suggests, an eclipse attack nature is to shadow honest nodes, so they are untraceable in the network. A malicious attacker control all incoming links to honest nodes in the network and thus makes the unreachable node [3].
- **Attack on Smart Contracts:** As smart contracts are hard coded in languages like Solidity, Go, and others, the programming constructs in the code make the code open and vulnerable for target attackers [14]. Irreversible, i.e., tamper-resistance, becomes a challenge for attackers because they can't introduce errors or bugs. An attack named decentralized autonomous organization (DAO) in 2016 was made on the Ethereum blockchain, leading to forking [40]
- **Privacy Leakage using Key:** Adversaries can control users' accounts by stealing the private key by capturing physical nodes or traditional network attacks [11].
- **DDoS Attack:** Attacker can introduce a coordinated attack intended to exhaust the network capacity, such that availability is compromised [58,48].
- **Programming Frauds:** Attackers do modification in code or exploit fraud that can lead to compromising privacy in blockchain [30].

As discussed above, attacks like privacy leakage using physical nodes may lead to critical conditions in applications based on healthcare devices, so the issues related to privacy become a key challenge in integration [74]. Also, using PoW in the IoT environment can lead to 51% of devices being captured by an attacker and the significant cause of loss of control in IoT applications. So based on the attacks mentioned above, we classified some challenges in integration.

3.4 | Challenges in IoT-Blockchain Integration

We present significant challenges for better performance and the reliable security of blockchain with IoT based on the study of consensus mechanisms and security requirements of IoT [14,50].

- **Scalability:** Scalability refers to the effect on network performance when the size of the blockchain network expands. In a practical scenario, many IoT devices must communicate simultaneously through the system. Currently, employed research doesn't have a highly scalable framework that also satisfies throughput and latency requirements [19].
- **Increasing Throughput:** Many devices are needed in an IoT network to communicate, requiring a high-throughput system simultaneously. Improved performance typically in existing implementations reduces scalability that would not be ideal [34].
- **Data Privacy:** In a blockchain network, different use-cases like healthcare [75], fake news [76], and record management [77] shares critical and sensitive data, which is highly confidential and shareable among domain stakeholders only. As the data sharing and access rules apply to the underlying smart contracts, the privacy-preserving rules should validate that

data leakage is not possible by the contracts. A private or consortium blockchain with defined privacy rules and a consensus mechanism in IoT ecosystems solves these issues. On the downside, however, it tends to make the network more centralized, which violates the fundamental decentralized characteristic of blockchain networks. Thus, modern IoT networks employ an optimal mix and match of centralization in sub-components and decentralization in the whole ecosystem [15].

- **Security:** In IoT networks, security attacks are mainly targeted toward disclosure, alteration, and denial of services. A functionally complete IoT network should be prone to a majority of attack vectors. Common avoidance measures require sending data in an encrypted form whenever possible through lightweight encryption mechanisms. Any authorized entity should share certificates whenever possible, and authentication of plug-and-play IoT devices is essential [24,22].

- **Latency Reduction:** In IoT networks, millions of devices might communicate in real time, and many applications have tight constraints on delay parameters. For example, vehicular networks require real-time route information to prevent undesirable conditions like collisions and congested routes. Thus, the communication latency should be minimal, even with the scaling of IoT devices [17]. Moreover, the shared data is critical, and thus recent solutions include federated learning (FL) with IoT that forms local learning models in vehicular communication [78].

- **Overcoming Limited Capacity:** In a blockchain network, to assure consensus, nodes are expected to maintain a ledger copy. As IoT ecosystems are resource-constrained, thus it is not possible to retain the copy ledger at each node [19]. In such cases, a lightweight consensus mechanism should be deployed at the expense of security costs. However, the balance of resource requirement against security should be balanced based on application requirements [26,79].

3.5 | Comparison of Blockchain Implementation Platforms

Various platforms are introduced to implement functionalities of blockchain, such as hyperledger-fabric [72], Ethereum [45], IOTA [63] after the very first bitcoin. In **TABLE** 6, we compared various parameters of those platforms concerning smart contract support, consensus, security, and performance requirements in IoT.

4 | RESEARCH GAPS, FINDINGS AND FUTURE DIRECTIONS

We have seen various consensus and smart contract-related challenges in the previous section. To incorporate these issues and challenges with IoT networks, we elaborate on unaddressed issues and research findings that can be emerging directions in future research towards integrating blockchain in the IoT ecosystem.

- **IoT-centric Consensus Mechanism:** The Internet of Things combines sensor devices and mobile devices, so they have different data formats for storage and process. Thus, it becomes necessary to have a consensus that deals with dynamic compositions or is based on validation rules instead of formats to achieve good transaction throughput and data privacy. The study also observed that most consensus has digital currency for transactions. According to requirements, it should be optional in resource-constrained IoT devices except for some critical applications where economic involvement is much needed.

- **Location-based Consensus Requirements:** In location-based ecosystems, like vehicular networks, sensor nodes measure road dimensions and spatial requirements based on network density. Thus, consensus mechanisms should deploy an effective mix of spatial and temporal requirements, as the effective topology varies with time [81]. At the same time, effective machine-learning mechanisms might improve the network's capacity, and machine-learning algorithms might interpret historical data to improve accuracy.

- **Blockchain Editing:** In bitcoin tracking business transactions, the cumulative volume has risen to more than 150 GB in the present scenario, while the genesis block was in 2009. In a blockchain, we can measure the chronology of the added transactions, which becomes very useful in supply-chain operations. In a blockchain, tampering in data is not allowed; however, through redactable blockchains, tampering becomes possible in a subset of block structures.

TABLE 6 Comparison of Blockchain Platforms

Platforms	Hyperledger [80,72]	Ethereum [45]	IOTA [62]	Bitcoin [40]
Category	Permissioned, Private and, Consortium	Permission-less, Private, Public Consortium	Permission-less, Not a Blockchain	Permission-less
Digital Currency	None	Ether	None	Bitcoin
Trustless Environment	Partial: Based on Trusted Validator Nodes	Yes	Yes	Yes
Type of Consensus	SIEVE, PBFT, Pluggable	PoW, PoS, Casper, DPoS,	DAG-based	PoW
Finality	Yes	No	No	No
Forks	No	Yes	-	Yes
Transaction Fees	Optional	Yes	No	Yes
Smart Contract	Yes	Yes	-	No
Throughput (TPS)	> 3000 and Dependent upon total nodes	8-10 TPS	Variable	7-8 TPS
Transaction Confirmation Time	Less than other Platforms	15-20 seconds	-	10 Minutes for a Block and 60 minutes for a single Confirmation
Data Confidentiality	Yes	No	No	No
User Authentication	Yes, Enrollment Certificates by CA	Yes, Digital Signature	Yes, Digital Signature	Yes, Digital Signature
Device Authentication	No	No	Partial	No
Transaction Authentication	Yes	Yes	Yes	Yes
Identity Management	Yes	No	No	No
Key Management	Yes	No	No	No
Application Domains	Multiple, Consortium for IoT	Multiple	Multiple	Financial Applications

- **Lightweight Encryption in blockchain-enabled IoT:** Some of the previous work shows that some standard communication protocols are generally used for device-to-device communication in IoT ecosystems. While IoT devices can only opt for lightweight encryption-decryption for data and transaction protection, enhancement and new development of lightweight encryption algorithms are needed. Designing and developing a consensus framework in the combined (centralized and decentralized) mining context is also vital.
- **Allocation of Energy Consumption Resources:** There are various approaches to preventing energy consumption in blockchain-based systems, and they are still inadequate compared to the performance of lower-end devices. High-processing blockchain nodes to enhance IoT systems' resilience directly affect the overall device energy consumption. If only a few blockchain nodes and lower complexity for the mining algorithm are adapted, they can run moderated.
- **Secure Smart Contracts with IoT-centric Verification:** Smart contracts are blockchain Scripts, and because of their flexibility, they are so efficient. SC can reliably protect and store data, limit access to the data to only the appropriate parties, and program it to use it inside a logical service operation between the stakeholders. The use of smart contracts in IoT systems can provide an effective means of enhancing IoT data privacy and security.
- **Resiliency to Mixed Attacks:** As seen in this study, there are several attacks on blockchain-based IoT. The attacks can be divided into two categories: one is application-free, i.e., each protocol handles a subset of attacks, and then each application-free attack is tackled using a different security mechanism. Another one is application dependent, where they are unique to each program and are thus easily considered in securing the application.
- **IOTA Adaption:** It uses distributed' Tangle' public ledger with underlying structure DAG. IOTA provides a smooth, stable, lightweight, and fee-free real-time transaction. It is a decentralized currency and open-source, mainly designed for IoT. So, this can potentially solve the decentralization for smart applications but is still under development.

Based on the above-identified area in the integration of blockchain in IoT, we have formulated some possible directions that are less explored and need attention in the future. **TABLE** 7 shows the research opportunities with a particular area in integration.

TABLE 7 Possible Research Opportunities based on Integrating Blockchain in IoT

Area of Research in Blockchain-enabled IoT	**Possible Research Directions / Opportunities**	
IoT-centric Consensus	RD1	How to design and develop more IoT-Centric consensus with specified validation rules that makes it fast?
Location-based Consensus	RD2	How to use geographical information with delay-sensitive content to make consensus more content-oriented?
	RD3	What strategies can be applied to protect the attacks in nearby node consideration in case of temporal sensitivity?
Editing in Blockchain	RD4	How to make intelligent editing that prevents data loss and gives strong resilience against modification by attackers?
Lightweight Encryption	RD5	Design and Develop lightweight encryption using time-delay tradeoff
Resource and Energy consumption	RD6	Develop attribute-based encryption that reduces the overhead of computing in IoT-Blockchain combination.
Secure Smart contract	RD7	Will smart contracts execute any event in the IoT system work appropriately with billions of devices?
	RD8	How well the smart Contract should react to change IoT environmental factors are as complicated as dynamic?
	RD9	What platform is suitable for enforcing smart IoT contracts?
Attacks Models	RD10	How to develop a security solution that can be immune to various attacks while considering implementations feasibility for the solution, particularly for low-resource IoT devices.
New platform adoption (IOTA)	RD11	What are the best technologies for decentralization? Blockchain or IOTA for IoT?
	RD12	How to solve significant barriers that challenge IOTA, such as storage and associated transaction selection?

5 | CASE STUDY: SMART CONTRACT DRIVEN BLOCKCHAIN APPROACH FOR SMART HEALTHCARE

The comprehensive architecture of the case study for the proposed solution using blockchain is presented in this section. We developed a smart healthcare network framework by integrating IoT and blockchain. The value of using IoT sensors is that they enable gathering data and making it automatic to exchange. On the other hand, the network benefits from blockchain encryption and smart contracts to achieve integrity, safety, traceability, and authentication. These features will allow patients to have complete control over their records.

Some of the current research and development strategies for combining blockchain with IoT-based healthcare lie in the scale of the blocks. A block on a blockchain holds transactions that are brief record-keeping statements. Putting whole health records on a blockchain will increase the entire chain's size, requiring more data at each node. With this variation, the challenge is those sensor devices used for smart healthcare have low processing power and less storage capacity; thus, it is challenging to incorporate them into a blockchain. Additionally, they often don't support the deployment of a thin client to join the blockchain network[82].

According to some studies, sensor data could be sent to the blockchain using the gateway as a node[83]. But, we also need help to protect the connection between the machines and the gateway (i.e., mobile or laptop) of the patient. For example, in this case, malicious devices may be added by a third party to send false data or stop the the functionality of gateway. The proposed case study relies on improving security at this stage. The alternative is registering each new device with its owner in the blockchain. The unknown device will be unable to access the platform until the owner registers it and authorizes it[84]. The system for IoT-blockchain-based healthcare is explained via **FIGURE** 7. We can split it into four components: Blockchain, Connected smart devices, Smart contracts, and Healthcare professionals.

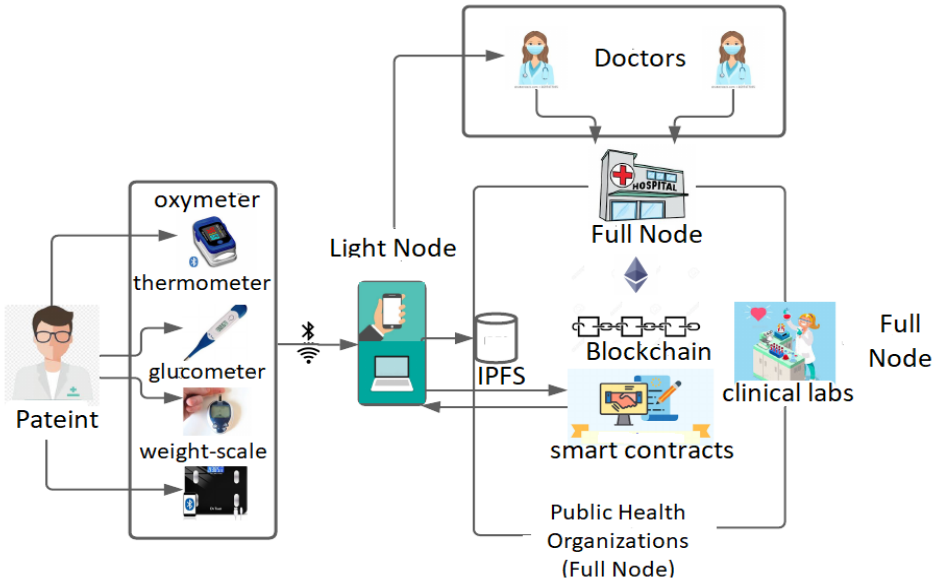

FIGURE 7 System Model for Blockchain based Smart Healthcare

5.1 | Components of Proposed System

This subsection elaborates on the different components for handling smart healthcare applications.

5.1.1 | Connected Smart Devices

Smart healthcare shows the categorization of devices into two ways; the first involves medical instruments, sensors, and fitness trackers that capture patient health information, such as oxygen level, weight, temperature, heart rate, glucose level, and other required remote patient tracking interventions. These devices gather data and immediately share them via gateways (i.e., smartphones or light nodes) with health professionals. The second form of connected devices is a mobile device used as an interface between the blockchain network and sensor-based medical devices. It utilizes an application to manage, encrypt, and route information from smartphones to an off-chain database that registered hospitals and healthcare professionals can access. By using this application, the patient would be able to communicate with their health professionals and devices. It will also give or withdraw access and approvals and connect or delete a device that will add/remove transactions submitted and deposited in the blockchain network through the suggested application.

Since the patient is still on the go and won't always be at home, using the smartphone as a gateway is an excellent idea. So we need a trustworthy gadget that can follow him everywhere—at home, at work, and when he's on the road.

5.1.2 | Blockchain

A P2P distributed file system maintains off-chain storage (IPFS) where patients can encrypt and store their messages, generating the hash from the blockchain. Patients can choose whether or not to allow permission to all parties. They also have the right to select which details to keep available and for whom. The information can be obtained by all health agencies while preventing private data which is encrypted. Here, each patient is recognized by his public key (i.e., ID). Healthcare professionals must access such details in case of an incident. The secret-sharing procedure enables each patient to gather this data prior to the encryption and distribution of the decryption key. The medical practitioner may then arrange for one or more family members of the patient to give the decryption key so that this information could be identified[85].

5.1.3 | Smart Contracts

Smart contracts are programs generated in the blockchain network, converted into byte code, and deployed. A unique address specifies each smart contract and can be activated by sending a transaction to this address. The implementation of smart contracts would enable the creation of a traceability log by recording each data manipulation. Additionally, it can be used for adding or removing devices, granting or denying access, defining policies, and verifying authentication.

5.1.4 | Healthcare Professionals Team

Entities such as public health agencies, disease care centers, scientists, clinical labs, hospitals, and healthcare professionals, in general, may be involved as a part of a medical team. Through a semi-permissioned blockchain, these organizations would be linked and provide access to data. This blockchain will allow health professionals to follow their patients' health and gather information to use research or statistics.

5.2 | Functions of Proposed System

In this subsection, we explain the functionality of the proposed case study in detail.

5.2.1 | User Device Registration:

A blockchain add transaction is used in this stage by the patient to register each new device. A unique set of values will define each device, its identifier (represented by its identity, i.e., MAC address), and identifiers of its holders (Ethereum public address of the patient) as shown in **FIGURE** 8. Thus, apart from the patient, no one can connect a device. The patient can fully control his gadgets and be guarded against malicious devices.

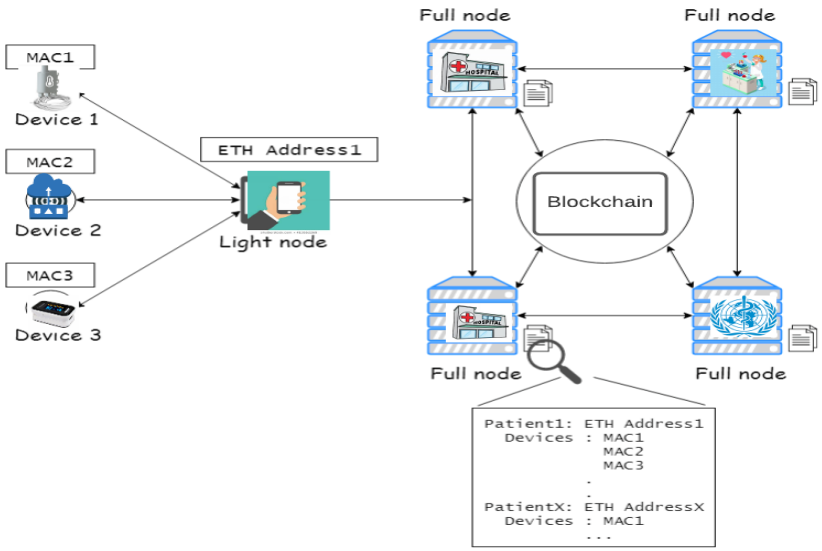

FIGURE 8 Device Registration in Smart Healthcare via Blockchain Network

5.2.2 | Decentralized Application (DApp)

A DApp is a framework that runs on a P2P network without needing a central authority. Because of its open nature, it has several characteristics that make it fascinating. It can be written in web scripts on the client-side (front end). Rather than linking this side to a backend of the server, we connect it to a blockchain and then link it to smart contracts. The patient can use the device interface to make separate transactions, as shown in **FIGURE** 9.

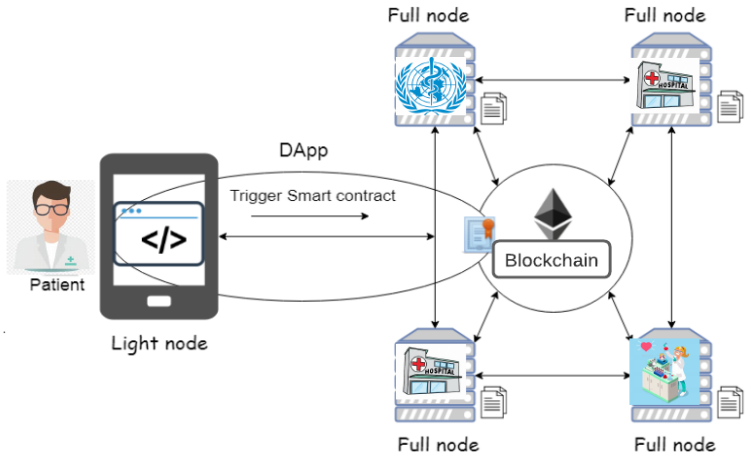

FIGURE 9 DApp and Smart Contract with Blockchain for Smart Healthcare

5.2.3 | Data Encryption and Decryption

Data would be encrypted by the patient before being stored in the IPFS. A smart contract will check a party's eligibility once it sends a transaction through the DApp requesting access to data. The patient provides the decryption key encrypted with the permitted party's public key if they have access authorization. The authorized party will use its private key to decrypt the message in order to obtain the decryption key and gain access to the data.

5.2.4 | Healthcare Transactions

By creating a scan code, healthcare professionals can add and register their patients in the blockchain. The Ethereum address of the doctor and the blockchain network details will be found on this scan code. Suppose the patient is registered in the blockchain. In that case, it can do various operations, such as adding or removing devices, granting or revoking permissions to other nodes, establishing policies, and accessing its data. To start these transactions and store them in the blockchain for traceability, DApp will activate smart contracts. Finally, the patient is added and reported by his physician in the blockchain.

5.3 | System Workflow

The workflow of the system would infuse a consortium blockchain setup. The advantage of using a consortium setup would allow authorized stakeholders only to access the system and perform modifications. Moreover, it would exert greater control on access rights and allow lightweight consensus to add blocks to the system. Thus, system managers such as care providers and patients could keep their sensitive data intact and would allow no disclosure of chronological events. The consensus setup would form a selection committee where miners would be selected on a voting basis, with authorized signatures, before writing to a block.

The consortium setup would ensure that collusion attacks are not possible while maintaining the decentralized theme of the system. Fake transactions cannot be instilled, and heavy resource-intensive techniques like Proof-of-Work would be avoided. The proposed contracts would be highly modular and customizable per the application requirements. The contract architecture would be hierarchical, where sub-functions would take data from individual patient histories and perform operations based on customized threshold values. Based on this, the deployed contract is non-editable, and for instilling changes in a particular contract, the previous contract changes would be locked and timestamped. New changes would then be introduced (similar to version controlling in git systems). Thus, this flexible system makes it possible to introduce changes in the contract without disrupting the other running services at the backend. **FIGURE** 10 shows the flow of system.

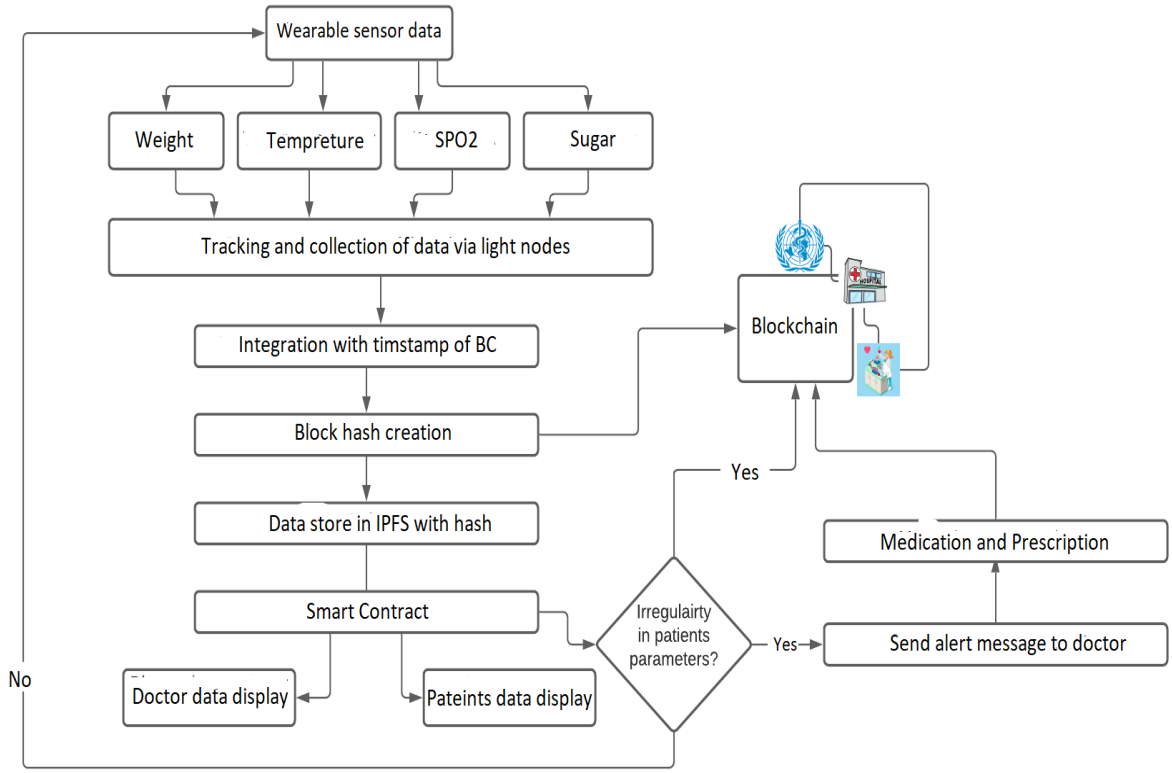

FIGURE 10 Flow Diagram of Blockchain Smart Contract based IoT-enabled Healthcare

5.4 | Implementation Aspects

The implementation aspects are simple to control. The contracts are designed using the Ethereum solidity language on consortium chain setup. **FIGURE** 11 demonstrates the conceptual flow of smart contracts designed to manage records. In the flow, the primary contract, termed as SH-Contract-Caller, would call the underlying IoT device to manage and send the data to the contract, and then based on access rules, the contract functions would be executed. The contracts (or chain codes) are executed in isolated docker containers to allow isolation. For example, if we consider the temperature measurement of the patient from the IoT sensor, the system would call the Temp-contract call. This would further invoke the SH-Contract-Caller object, which has the temp-data-function() as a primary call. The thresholds for the temperature value (minimum and maximum) are passed as initializers and sent to relevant functions.

The data is then analyzed by the contract, and the parameters are sent to the analyze () function. Thus, sub-contract modularity leverages only relevant parts of the contract to execute, saving the power of the nodes not under consideration. The sub-transactions would write the data in the main on-chain and would notify the associated nodes of the change. In case of alert functions, the contract would notify the concerned authority, like the hospital, to take immediate action on the patient wearing the smart device (for example, priority tasks to put an oxygen cylinder, give medical treatment, medicines, and measure the blood pressure of the patient).

5.5 | Comparative Analysis

Blockchain has been a comparatively new invention compared to conventional systems based on central servers. System workflow, like our proposed solution, is distinct from current approaches that perform similar purposes. Blockchain depends primarily on more conventional connectivity and data storage models, such as cloud processing and relational databases.

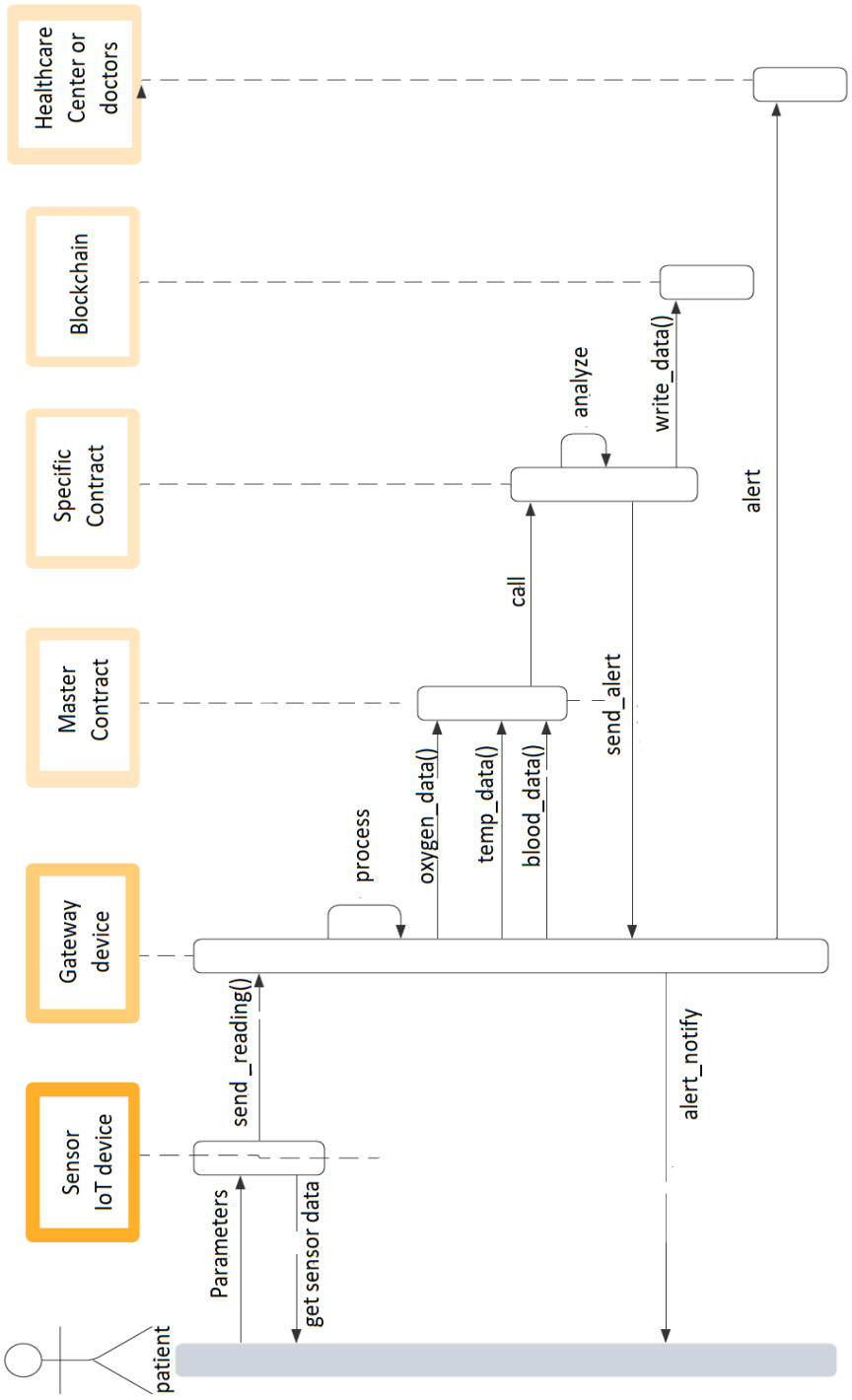

FIGURE 11 Smart Contract Execution Sequence for Proposed IoT-based Smart Healthcare Integrating Blockchain

5.6 | Security analysis

We presume that using cryptography, IP protocols are protected, and we do not add any more.

- Our approach uses device registration, as mentioned in a case study, that offers local-level protection such that new device addition by an attacker is eliminated. It is possible to trigger smart contract-based user registration, and only authorized devices can monitor patients' reading. Thus the malicious node does not eavesdrop on data, and message attack duplication can be stopped.
- Authentication for parties that might be able to access the data inside the smart system must be present (i.e., the patients would have read rights on their data, and based on their permission, the healthcare stakeholders can make changes in the contract).
- To make a block legitimate, the proposed blockchain network makes it mandatory to reach the most signatures from consortium members, keeping the database from being exploited by one party. In addition, the blockchain's viewing rights are limited to only registered parties (patients and healthcare professionals). For the patient and the healthcare professional, the blockchain database recording the transactions often acts as a separate security means. An accurate record may be helpful in conflict resolution and reporting procedures.
- The details on the blockchain, as suggested, includes only transaction information and not sensitive health data. Also, the patients' account addresses are anonymized since data is not readily connected to a single entity, thereby protecting anonymity.

6 | CONCLUSION AND FUTURE WORK

The emerging blockchain can effectively address challenges, such as decentralization, fault tolerance, anonymity, and transaction integrity, due to its underlying concepts of consensus, smart contract, and cryptographic properties. This paper focused on how blockchain properties can be used to address IoT performance and security requirements. We explored the various consensus mechanism and smart contract concepts and compared them with necessities and applicability in resource-constrained IoT networks. By looking into blockchain-enabled IoT, we identified some of the challenges in integration. Further, we stated some research directions that can help overcome current issues based on the current state of the art. The presented case study shows how blockchain is helpful in smart healthcare based on IoT configuration for real-time data security and privacy.

In the future, we would design privacy-preserving mechanisms to synergize with the consortium setup. They would propose lightweight consensus mechanisms with sleep mechanisms to save the energy requirements of the constrained IoT nodes.

DATA AVAILABILITY STATEMENT

There is no data available to carry out this research.

CONFLICT OF INTEREST

Authors want to declare that at the time of submission of this article there is no conflict of Interest.

References

1. Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems* 2018; 82: 395–411.
2. Ahanger TA, Aljumah A. Internet of Things: A comprehensive study of security issues and defense mechanisms. *IEEE Access* 2018; 7: 11020–11028.

3. Ali MS, Vecchio M, Pincheira M, Dolui K, Antonelli F, Rehmani MH. Applications of blockchains in the Internet of Things: A comprehensive survey. *IEEE Communications Surveys & Tutorials* 2018; 21(2): 1676–1717.

4. Frustaci M, Pace P, Aloi G, Fortino G. Evaluating critical security issues of the IoT world: Present and future challenges. *Internet of Things Journal* 2017; 5(4): 2483–2495.

5. Patel SB, Kheruwala HA, Alazab M, et al. BioUAV: Blockchain-Envisioned Framework for Digital Identification to Secure Access in next-Generation UAVs. In: DroneCom '20. Association for Computing Machinery; 2020; New York, NY, USA: 43–48

6. Zhou W, Jia Y, Peng A, Zhang Y, Liu P. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *Internet of Things Journal* 2018; 6(2): 1606–1616.

7. Hassan WH, others . Current research on Internet of Things (IoT) security: A survey. *Computer Networks* 2019; 148: 283–294.

8. Nandy T, Idris MYIB, Noor RM, et al. Review on Security of Internet of Things Authentication Mechanism. *IEEE Access* 2019; 7: 151054–151089.

9. Sanghvi J, Bhattacharya P, Tanwar S, Gupta R, Kumar N, Guizani M. Res6Edge: An Edge-AI Enabled Resource Sharing Scheme for C-V2X Communications towards 6G. In: ; 2021: 149-154

10. Trnka M, Cerny T, Stickney N. Survey of Authentication and Authorization for the Internet of Things. *Security and Communication Networks* 2018; 2018.

11. Ismail L, Materwala H. A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry* 2019; 11(10): 1198.

12. Forouzan BA. *Cryptography & network security*. McGraw-Hill, Inc. . 2007.

13. Bodkhe U, Bhattacharya P, Tanwar S, Tyagi S, Kumar N, Obaidat MS. BloHosT: Blockchain Enabled Smart Tourism and Hospitality Management. In: ; 2019: 1-5

14. Sengupta J, Ruj S, Bit SD. A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications* 2020; 149: 102481.

15. Zhang R, Xue R, Liu L. Security and privacy on blockchain. *ACM Computing Surveys (CSUR)* 2019; 52(3): 1–34.

16. Wang S, Ding W, Li J, Yuan Y, Ouyang L, Wang FY. Decentralized autonomous organizations: concept, model, and applications. *IEEE Transactions on Computational Social Systems* 2019; 6(5): 870–878.

17. Danzi P, Kalør AE, Stefanović Č, Popovski P. Delay and communication tradeoffs for blockchain systems with lightweight IoT clients. *IEEE Internet of Things Journal* 2019; 6(2): 2354–2365.

18. Hang L, Kim DH. Design and implementation of an integrated iot blockchain platform for sensing data integrity. *Sensors* 2019; 19(10): 2228.

19. Banerjee M, Lee J, Choo KKR. A blockchain future for internet of things security: a position paper. *Digital Communications and Networks* 2018; 4(3): 149–160.

20. Bhattacharya P, Tanwar S, Shah R, Ladha A. Mobile Edge Computing-Enabled Blockchain Framework—A Survey. In: Singh PK, Kar AK, Singh Y, Kolekar MH, Tanwar S., eds. *Proceedings of ICRIC 2019*Springer International Publishing; 2020; Cham: 797–809.

21. Bang AO, Rao UP, Visconti A, Brighente A, Conti M. An IoT Inventory Before Deployment: A Survey on IoT Protocols, Communication Technologies, Vulnerabilities, Attacks, and Future Research Directions. *Computers & Security* 2022; 123: 102914. doi: https://doi.org/10.1016/j.cose.2022.102914

22. Roy S, Ashaduzzaman M, Hassan M, Chowdhury AR. Blockchain for IoT security and management: current prospects, challenges and future directions. In: IEEE. ; 2018: 1–9.

23. bitcoin.pdf. https://bitcoin.org/bitcoin.pdf; . (Accessed on 07/06/2021).

24. Conoscenti M, Vetro A, De Martin JC. Blockchain for the Internet of Things: A systematic literature review. In: IEEE. ; 2016: 1–6.

25. Alharby M, Aldweesh A, Moorsel vA. Blockchain-based smart contracts: A systematic mapping study of academic research (2018). In: IEEE. ; 2018: 1–6.

26. Dorri A, Kanhere SS, Jurdak R. Towards an optimized blockchain for IoT. In: IEEE. ; 2017: 173–178.

27. Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: The case study of a smart home. In: IEEE. ; 2017: 618–623.

28. Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems* 2018; 88: 173–190.

29. Hammi MT, Hammi B, Bellot P, Serhrouchni A. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security* 2018; 78: 126–142.

30. Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J. Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal* 2018; 6(2): 1594–1605.

31. Ouaddah A, Mousannif H, Elkalam AA, Ouahman AA. Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks* 2017; 112: 237–262.

32. Patel NS, Bhattacharya P, Patel SB, Tanwar S, Kumar N, Song H. Blockchain-Envisioned Trusted Random Oracles for IoT-Enabled Probabilistic Smart Contracts. *IEEE Internet of Things Journal* 2021; 8(19): 14797-14809. doi: 10.1109/JIOT.2021.3072293

33. Ferrag MA, Derdour M, Mukherjee M, Derhab A, Maglaras L, Janicke H. Blockchain technologies for the internet of things: Research issues and challenges. *IEEE Internet of Things Journal* 2018; 6(2): 2188–2204.

34. Dorri A, Kanhere SS, Jurdak R, Gauravaram P. LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *Journal of Parallel and Distributed Computing* 2019; 134: 180–197.

35. Biswas K, Muthukkumarasamy V. Securing Smart Cities Using Blockchain Technology. In: ; 2016: 1392-1393.

36. Moin S, Karim A, Safdar Z, Safdar K, Ahmed E, Imran M. Securing IoTs in distributed blockchain: Analysis, requirements and open issues. *Future Generation Computer Systems* 2019; 100: 325–343.

37. Cao B, Li Y, Zhang L, et al. When Internet of Things meets blockchain: Challenges in distributed consensus. *IEEE Network* 2019; 33(6): 133–139.

38. Developer Guides — Bitcoin. https://developer.bitcoin.org/devguide/; . (Accessed on 08/01/2021).

39. Ghayvat H, Pandya S, Bhattacharya P, et al. CP-BDHCA: Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare Clouds and Applications. *IEEE Journal of Biomedical and Health Informatics* 2022; 26(5): 1937-1948. doi: 10.1109/JBHI.2021.3097237

40. Tschorsch F, Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials* 2016; 18(3): 2084–2123.

41. Zhang S, Lee JH. Analysis of the main consensus protocols of blockchain. *ICT Express* 2020; 6(2): 93–97.

42. Abdelmaboud A, Ahmed AIA, Abaker M, et al. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* 2022; 11(4). doi: 10.3390/electronics11040630

43. Moinet A, Darties B, Baril JL. Blockchain based trust & authentication for decentralized sensor networks. *arXiv preprint arXiv:1706.01730* 2017.

44. Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang FY. Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 2019; 49(11): 2266–2277.

45. Ethereum for Developers | ethereum.org. https://ethereum.org/en/developers/; . (Accessed on 19/04/2020).

46. Hyperledger Fabric Model — hyperledger-fabricdocs master documentation. https://hyperledger-fabric.readthedocs.io/en/release-1.2/fabric_model.html#privacy; . (Accessed on 27/05/2021).

47. Yeow K, Gani A, Ahmad RW, Rodrigues JJ, Ko K. Decentralized consensus for edge-centric internet of things: A review, taxonomy, and research issues. *IEEE Access* 2017; 6: 1513–1524.

48. Yang Y, Wu L, Yin G, Li L, Zhao H. A survey on security and privacy issues in Internet-of-Things. *Internet of Things Journal* 2017; 4(5): 1250–1258.

49. Wang X, Zha X, Ni W, et al. Survey on blockchain for Internet of Things. *Computer Communications* 2019; 136: 10–29.

50. Salimitari M, Chatterjee M, Fallah Y. A Survey on Consensus Methods in Blockchain for Resource-constrained IoT Networks. *Internet of Things* 2020; 11: 100212. doi: 10.1016/j.iot.2020.100212

51. Lepore C, Ceria M, Visconti A, Rao UP, Shah KA, Zanolini L. A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS. *Mathematics* 2020; 8(10): 1782.

52. Xu LD, Lu Y, Li L. Embedding Blockchain Technology Into IoT for Security: A Survey. *IEEE Internet of Things Journal* 2021; 8(13): 10452-10473. doi: 10.1109/JIOT.2021.3060508

53. Uddin MA, Stranieri A, Gondal I, Balasubramanian V. A survey on the adoption of blockchain in IoT: challenges and solutions. *Blockchain: Research and Applications* 2021; 2(2): 100006. doi: https://doi.org/10.1016/j.bcra.2021.100006

54. Abdelmaboud A, Ahmed AIA, Abaker M, et al. Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics* 2022; 11(4). doi: 10.3390/electronics11040630

55. Tanwar S, Gupta N, Iwendi C, Kumar K, Alenezi M. Next Generation IoT and Blockchain Integration. *Journal of Sensors* 2022; 2022.

56. Li D, Deng L, Cai Z, Souri A. Blockchain as a service models in the Internet of Things management: Systematic review. *Transactions on Emerging Telecommunications Technologies* 2022; 33(4): e4139. e4139 ETT-20-0827.R1doi: https://doi.org/10.1002/ett.4139

57. Yu Y, Li Y, Tian J, Liu J. Blockchain-based solutions to security and privacy issues in the Internet of Things. *IEEE Wireless Communications* 2018; 25(6): 12–18.

58. Neshenko N, Bou-Harb E, Crichigno J, Kaddoum G, Ghani N. Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials* 2019.

59. Sicari S, Rizzardi A, Grieco LA, Coen-Porisini A. Security, privacy and trust in Internet of Things: The road ahead. *Computer networks* 2015; 76: 146–164.

60. ByzCoin: Securely Scaling Blockchains. https://hackingdistributed.com/2016/08/04/byzcoin/; . (Accessed on 07/03/2021).

61. Tendermint Core. https://docs.tendermint.com/master/introduction/introduction.html#consensus-overview; . (Accessed on 07/07/2021).

62. iota143.pdf. https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf; . (Accessed on 22/07/2021).

63. IOTA Ecosystem. https://ecosystem.iota.org/; . (Accessed on 27/07/2021).

64. How IOTA works | Understanding IOTA | Getting Started | IOTA Documentation. https://docs.iota.org/docs/getting-started/1.0/understanding-iota/overview#the-tangle; . (Accessed on 07/07/2021).

65. Verma A, Bhattacharya P, Madhani N, et al. Blockchain for Industry 5.0: Vision, Opportunities, Key Enablers, and Future Directions. *IEEE Access* 2022; 10: 69160-69199. doi: 10.1109/ACCESS.2022.3186892

66. Bodkhe U, Mehta D, Tanwar S, Bhattacharya P, Singh PK, Hong WC. A Survey on Decentralized Consensus Mechanisms for Cyber Physical Systems. *IEEE Access* 2020; 8: 54371-54401. doi: 10.1109/ACCESS.2020.2981415

67. Tian H, Ge X, Wang J, Li C, Pan H. Research on distributed blockchain-based privacy-preserving and data security framework in IoT. *IET Communications* 2020; 14(13): 2038-2047. doi: https://doi.org/10.1049/iet-com.2019.0485

68. Alkhateeb A, Catal C, Kar G, Mishra A. Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review. *Sensors* 2022; 22(4). doi: 10.3390/s22041304

69. Szabo N. The idea of smart contracts. *Nick Szabo's Papers and Concise Tutorials* 1997; 6.

70. Luu L, Chu DH, Olickel H, Saxena P, Hobor A. Making smart contracts smarter. In: ; 2016: 254–269.

71. Rafati Niya S, Schiller E, Stiller B. *Architectures for Blockchain-IoT Integration 1*ch. 13: 321-344; John Wiley & Sons, Ltd . 2021

72. hyperledger-fabricdocs Documentation. https://buildmedia.readthedocs.org/media/pdf/hyperledger-fabric/latest/hyperledger-fabric.pdf; . (Accessed on 06/05/2021).

73. Restuccia F, Kanhere SD, Melodia T, Das SK. Blockchain for the Internet of Things: present and future. *arXiv preprint arXiv:1903.07448* 2019.

74. Bhattacharya P, Mehta P, Tanwar S, Obaidat MS, Hsiao KF. HeaL: A blockchain-envisioned signcryption scheme for healthcare IoT ecosystems. In: ; 2020: 1-6

75. Bodkhe U, Tanwar S, Bhattacharya P, Verma A. Blockchain Adoption for Trusted Medical Records in Healthcare 4.0 Applications: A Survey. In: Singh PK, Wierzchoń ST, Tanwar S, Ganzha M, Rodrigues JJPC., eds. *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security*Springer Singapore; 2021; Singapore: 759–774.

76. Bhattacharya P, Patel SB, Gupta R, Tanwar S, Rodrigues JJPC. SaTYa: Trusted Bi-LSTM-Based Fake News Classification Scheme for Smart Community. *IEEE Transactions on Computational Social Systems* 2021: 1-10. doi: 10.1109/TCSS.2021.3131945

77. Srivastava A, Bhattacharya P, Singh A, Mathur A, Pradesh U, Pradesh U. A systematic review on evolution of blockchain generations. *International Journal of Information Technology and Electrical Engineering* 2018; 7(6): 1–8.

78. Patel VA, Bhattacharya P, Tanwar S, Jadav NK, Gupta R. BFLEdge: Blockchain based federated edge learning scheme in V2X underlying 6G communications. In: ; 2022: 146-152

79. Bhattacharya P, Patel F, Tanwar S, Kumar N, Sharma R. MB-MaaS: Mobile Blockchain-based Mining-as-a-Service for IIoT environments. *Journal of Parallel and Distributed Computing* 2022; 168: 1-16. doi: https://doi.org/10.1016/j.jpdc.2022.05.008

80. Hyperledger_Arch_WG_Paper_1_Consensus.pdf. https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf; . (Accessed on 15/07/2021).

81. Bhattacharya P, Bodkhe U, Zuhair M, et al. Amalgamation of blockchain and sixth-generation-envisioned responsive edge orchestration in future cellular vehicle-to-anything ecosystems: Opportunities and challenges. *Transactions on Emerging Telecommunications Technologies*; n/a(n/a): e4410. doi: https://doi.org/10.1002/ett.4410

82. Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Sadoun B. HaBiTs: Blockchain-based telesurgery framework for healthcare 4.0. In: IEEE. ; 2019: 1–5.

83. Gupta R, Thakker U, Tanwar S, Obaidat MS, Hsiao KF. Bits: A blockchain-driven intelligent scheme for telesurgery system. In: IEEE. ; 2020: 1–5.

84. Rizzardi A, Sicari S, Miorandi D, Coen-Porisini A. Securing the access control policies to the Internet of Things resources through permissioned blockchain. *Concurrency and Computation: Practice and Experience* 2022; 34(15): e6934. doi: https://doi.org/10.1002/cpe.6934

85. Vora J, Nayyar A, Tanwar S, et al. BHEEM: A blockchain-based framework for securing electronic health records. In: IEEE. ; 2018: 1–6.