Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.063304

REVIEW

Blockchain Integration in IoT: Applications, Opportunities, and Challenges

Mozhgan Gholami[1], Ali Ghaffari[1,2,3,*], Nahideh Derakhshanfard[1], Nadir iBRAHIMOĞLU[4] and Ali Asghar Pourhaji Kazem[2]

[1]Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, 5157944533, Iran
[2]Department of Computer Engineering, Faculty of Engineering and Natural Science, Istinye University, Istanbul, 34396, Türkiye
[3]Department of Computer Science, Khazar University, Baku, AZ1096, Azerbaijan
[4]MSDC Department, Huawei R&D Center, İstanbul, 34768, Türkiye

*Corresponding Author: Ali Ghaffari. Email: a.ghaffari@iaut.ac.ir

Received: 10 January 2025; Accepted: 19 March 2025; Published: 16 April 2025

ABSTRACT: The Internet has been enhanced recently by blockchain and Internet of Things (IoT) networks. The Internet of Things is a network of various sensor-equipped devices. It gradually integrates the Internet, sensors, and cloud computing. Blockchain is based on encryption algorithms, which are shared database technologies on the Internet. Blockchain technology has grown significantly because of its features, such as flexibility, support for integration, anonymity, decentralization, and independent control. Computational nodes in the blockchain network are used to verify online transactions. However, this integration creates scalability, interoperability, and security challenges. Over the last decade, several advancements in blockchain technology have drawn attention from research communities and industries. Blockchain technology helps IoT networks become more reliable and enhance security and privacy. It also removes single points of failure and lowers the cost. In recent years, there has been an increasing amount of literature on IoT and blockchain technology applications. This paper extensively examines the current state of blockchain technologies, focusing specifically on their integration into the Internet of Things. Additionally, it highlights the benefits, drawbacks, and opportunities of recent studies on security issues based on blockchain solutions into categories. The survey examined various research papers from different types of publications. Also, a review of the other IoT applications has been included, focusing on the security requirements and challenges in IoT-based systems. Future research directions are gathered for the effective integration of Blockchain and IoT.

KEYWORDS: Internet of Things; blockchain; cybersecurity; privacy; security

1 Introduction

The IoT network comprises a variety of diverse nodes linked together via the Internet [1–4]. Four phases comprise the operation of the Internet of Things: first, sensors gather data; second, data is stored in the cloud; third, data analysis is performed, and the outcome is sent back to the device; and last, the device acts in response to the data it has received [5]. Data produced by the Internet of Things can be stored on multiple servers throughout a cloud infrastructure. Subsequently, a distributed approach to data processing and access is possible [6–8]. The number of internet-connected devices, including digital assistants, refrigerators, and lighting devices, is increasing daily [9].

By 2025, there will be 75 billion IoT devices worldwide, according to predictions [10,11]. The IoT is also estimated to produce 79.4 zettabytes of data by 2025. Devices in IoT networks collect, process, compute, and communicate with each other. The security of traditional network systems is threatened by the variety of

Internet of Things devices [12–15]. Sensitive data generated on the Internet of Things are attractive targets for attackers, exposing the entire network to security risks [16–19]. Internet of Things networks can be impacted by cyberattacks like ransomware and distributed denial of service (DDoS) [20]. Massive data production can cause a bottleneck on the Internet of Things, affecting the quality of services (QoS) [21–24]. One likely way to address this bottleneck issue is through blockchain architecture.

The integration of IoT and Blockchain is used in many fields, such as education, healthcare, smart homes, finance, agriculture [25], industry [26], and the environment [27]. Blockchain integration with the Internet of Things is a recent innovation that has boosted security. Every day, security threats produce newer forms of danger [28]. Consensus algorithms, processing speed and power, storage capacity, scalability, and other issues have arisen due to blockchain and IoT integration.

Blockchain is described by the National Institute of Standards and Technology [29]. A blockchain network is a decentralized/distributed network in which messages are broadcast through the network. In the context of IoT applications, cloud services often fail to guarantee the expected levels of data integrity and availability [30]. Although blockchain was initially created to record and confirm digital currency transactions, it is also used today to protect Internet of Things devices [31].

The communication protocols connected nodes use to exchange information have weak privacy and security [32]. Therefore, with the increasing popularity of the Internet of Things and the increase of smart devices, the current solutions are insufficient [33,34]. Blockchain technology can, therefore, be used to provide a secure, encrypted modular infrastructure [35,36]. Because blockchain is decentralized, most IoT experts today use it to protect against several cyber-attacks [37]. The security needs of the IoT can be met through the utilization of Blockchain technologies [38,39].

This paper contrasts with the current IoT security survey papers. It is preferable to split the chosen paper into two groups: IoT security survey papers and IoT security papers based on blockchain technology. Popular academic databases like IEEE Xplore, Web of Science (WoS), and Scopus were used to select the chosen papers. Based on the most current five-year reference (Google Scholar).

The primary goal of this survey is to determine the main challenges in IoT. In other words, find the challenges and proper solutions for them. The following is the contribution of this paper:

- An overview of blockchain types, architecture, and applications.
- This survey examines blockchain technology's distinct features and unresolved issues.
- Several methods for integrating blockchain technology with the IoT are identified and evaluated.
- The approach of integrating IoT with blockchain and the existing literature surveys are thoroughly compared.
- A thorough examination of blockchain applications across a range of IoT-related fields.
- The challenges, benefits, and problems of combining blockchain and IoT are discussed.

The rest of the paper is structured as follows: Section 2 discusses the historical background of the field and reviews the relevant literature. Section 3 provides an overview of IoT and blockchain technology architecture, applications, and challenges. Section 4 emphasizes IoT and blockchain integration. Section 5 describes the current challenges of IoT, Blockchain, and Integration and how to address these challenges. Section 6 offers suggestions for future directions and research areas. Finally, the paper concludes in Section 7. Fig. 1 presents the paper's instructions and roadmap, and the acronym.

Although there has been a lot of research on blockchain and IoT, a comprehensive survey that classifies, evaluates, and contrasts current solutions is essential. Researchers and practitioners must have a thorough understanding of how blockchain can improve the security, scalability, interoperability, and efficiency of the Internet of Things. This article aims to fill the gap by offering a thorough analysis of the

most recent developments in blockchain-based Internet of Things solutions, covering current frameworks, challenges, and future research directions. Researchers, developers, and industry professionals will find this a useful resource.

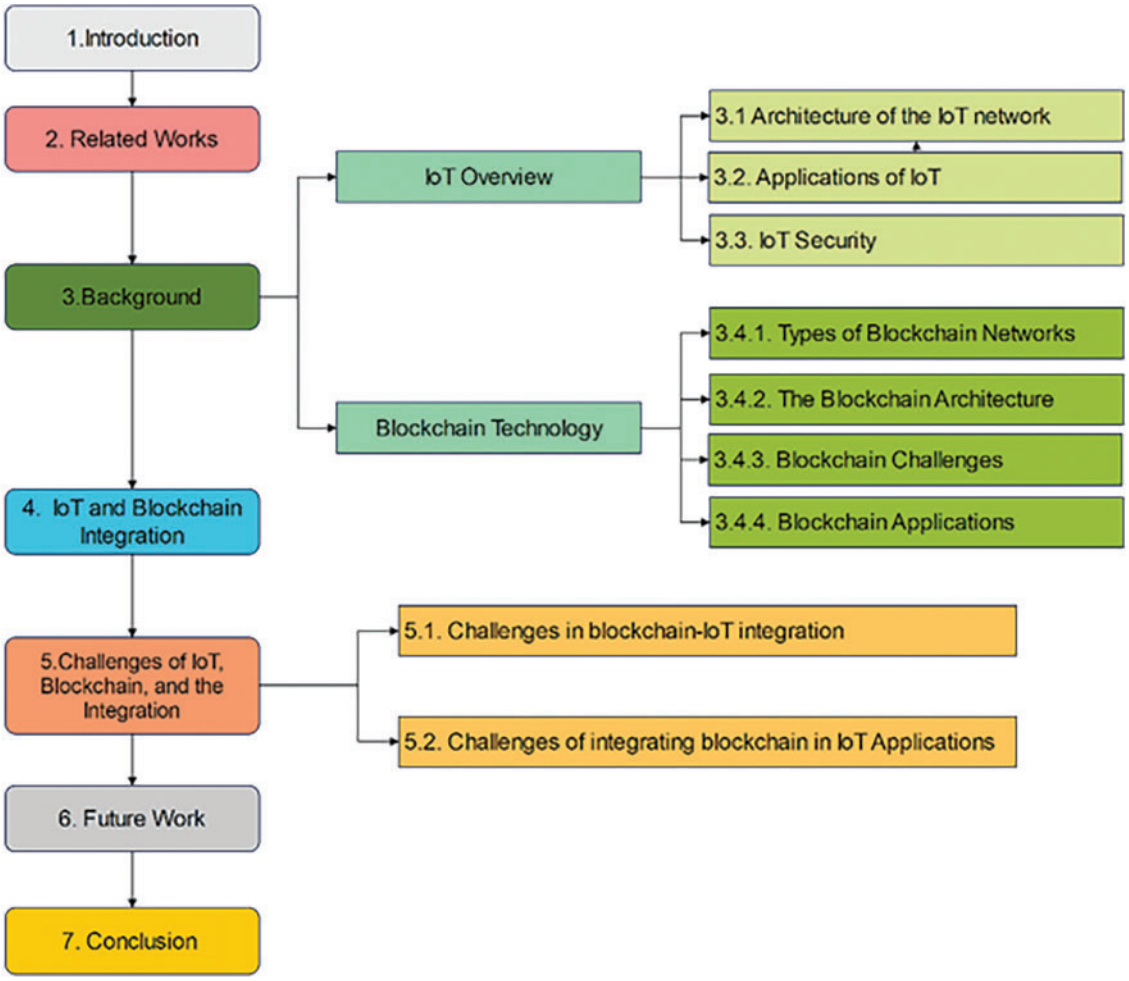

Figure 1: Survey road map

2 Related Works

Technological viewpoints have been applied to many recent studies on Blockchain, IoT, and related subjects. Several attempts have been made to produce review articles on this research topic. In [40], the authors describe the challenges of the IoT and the solutions that Blockchain provides to face these challenges. It also examines the integration of Blockchain with the Internet of Things and blockchain and introduces the architecture for integrating the Internet of Things and blockchain.

In [41], the authors assess the challenges in blockchain IoT applications to provide a proper analysis of how blockchain can improve the IoT. Reyna et al. conducted a study to explore the feasibility and research challenges associated with integrating blockchain technology with IoT. In [21,38], the authors also discussed the challenges of integrating the Internet of Things and Blockchain and pointed out their future research directions.

In [42], the authors presented a literature review on integrating blockchain technology into IoT. The authors provide a comprehensive overview of the existing Blockchain of Things (BCoT) research and discuss the possible applications of this new paradigm in various fields, such as healthcare, supply chain management, and energy management. This paper also highlights the technical challenges and open research directions in BCoT, such as scalability, consensus mechanisms, and regulatory issues. In addition to examining the challenges mentioned to bring blockchain technology and the Internet of Things together, the authors present BCoT architecture.

In [43], the authors presented a literature review of existing blockchain technologies focusing on their IoT applications. The authors identify the limitations of current blockchain technologies for Internet of Things applications by analyzing consensus protocols and data structures. This paper focuses on two typical structures for blockchain-based IoT applications: the IoT-involved blockchain and the blockchain as a service for IoT. It also discusses industrial blockchain-based IoT applications and projects. The authors analyze blockchain performance and IoT requirements, presenting critical challenges in integrating blockchain with IoT.

In [44], the authors looked at Blockchain technology in relation to the Internet of Things. A review of recent research on blockchain-based approaches to Internet of Things security is included. However, it only covers the technical aspects of blockchain technology, and there is no opinion on blockchain solutions in the real world. The difficulties and restrictions of combining blockchain technology with Internet of Things devices are also unmentioned. Blockchain, ML, and IoT technologies are concurrent, and Fazel et al. explore the exciting possibilities that result in [45]. This article did not address the scalability issues or potential constraints that could arise when implementing these technologies in large-scale IoT systems.

In [46], the authors investigate how blockchain can improve the Internet of Things security while also analyzing the risks associated with combining blockchain technology with the Internet of Things. They also present a framework for security problems that uses machine learning and game theory methods. By extracting historical data, machine learning aims to forecast potential future attacks, and game theory is utilized to update existing defense strategies, thereby optimizing defense strategies.

The main conclusions and input from earlier in-depth surveys that looked at the IoT and blockchain integration are summarized in Table 1.

Unlike the previous studies, our survey covers every facet of IoT security research, making it a unique contribution to the field. Their research focuses on the difficulties of using the Internet of Things. Although the potential of these technologies is discussed in each study, the literature contains case studies and empirical data that show how blockchain improves IoT security. Our survey closes this gap by combining these elements, adding a fresh perspective to the current literature and opening the door to investigating uncharted research territory. This survey is distinctive in covering works published through 2024 and includes a review of the most recent publications.

Consequently, our research and findings are grounded in the most recent developments and trends in the IoT space. As such, our work provides an up-to-date representation of cutting-edge research by compiling recent articles that have used blockchain technology in these networks.

Table 1: Recent survey comparisons

Article ref	Year	Blockchain-based features	IoT security	Blockchain-based IoT attacks	Blockchain-based IoT measures	Technical challenges	Future prospective	Main contribution	Limitations
[1]	2020	✓	✓	✓	×	✓	×	• Examines the security and privacy challenges in IoT applications to understand critical vulnerabilities of IoT security. • Examines how technologies like ML, AI, and Blockchain can be integrated into IoT systems to reduce threats and enhance security	Limited research focused on the practical implementation of these security solutions in real-world IoT applications
[21]	2018	×	✓	✓	×	✓	✓	Discusses the various blockchain-based IoT solutions and their current state of development	Discusses a small number of IoT and BC integration-related papers
[47]	2021	✓	✓	✓	×	×	×	• Pinpoints various security issues faced by IoT systems, and highlights how blockchain technology can effectively resolve these issues • Explores potential methods for integrating blockchain into IoT systems	It does not propose specific solutions or frameworks to address scalability issues effectively

(Continued)

Table 1 (continued)

Article ref	Year	Blockchain-based features	IoT security	Blockchain-based IoT attacks	Blockchain-based IoT measures	Technical challenges	Future prospective	Main contribution	Limitations
[38]	2023	✓	×	×	✓	✓	✓	• Presents the basic ideas of blockchain technology, including its features, workflow, and various application • Discusses the benefits and drawbacks of blockchain IoT convergence • Examines advantages and challenges posed by the integration of blockchain with IoT technologies	• Many solutions presented are theoretical and not backed by real-world implementations, making their practical applicability questionable • Some solutions are focused on specific applications, making them less generalizable to other IoT contexts • The implications of hardware constraints and the appropriateness of various consensus mechanisms for lightweight IoT devices are not adequately addressed

(Continued)

Table 1 (continued)

Article ref	Year	Blockchain-based features	IoT security	Blockchain-based IoT attacks	Blockchain-based IoT measures	Technical challenges	Future prospective	Main contribution	Limitations
[41]	2018	✓	✓	✓	×	✓	✓	• Compares the performance of different blockchain solutions in the context of IoT devices • Examines the features of blockchain technology and its unresolved issues • Evaluating various approaches to blockchain and IoT integration • Provides an overview of existing blockchain–IoT platforms and applications	• Challenges of integrating blockchain solutions with IoT frameworks and infrastructures have not been sufficiently addressed • The compatibility of different blockchain platforms with various IoT systems not mentioned
[42]	2019	✓	×	×	✓	✓	✓	• Provide an overview of the integration of Blockchain technology with IoT • Highlighting its potential to address critical challenges, related to security and privacy • Identifies several key issues in the development of Blockchain for IoT applications, including energy efficiency, security, privacy concerns, throughput and latency challenges, and usability	• Lack of industry-specific case studies or applications of Blockchain across various sectors. • Lack of analysis on security threats specific to Blockchain and IoT • Fails to sufficiently address the technical limitations of Blockchain technology, including transaction speed, data throughput, and consensus mechanisms

(Continued)

Table 1 (continued)

Article ref	Year	Blockchain-based features	IoT security	Blockchain-based IoT attacks	Blockchain-based IoT measures	Technical challenges	Future prospective	Main contribution	Limitations
[43]	2019	✓	×	×	✓	✓	✓	• Presents current blockchain technologies and their potential applications in IoT systems • Covers various consensus mechanisms, data structures, and scalability solutions pertinent to IoT • Highlights challenges of integrating blockchain technology into IoT networks, including issues related to data management, scalability, and security	Interoperability issues between blockchain systems and IoT technologies are not adequately addressed
[44]	2024	✓	✓	×	✓	✓	✓	• Explains how blockchain uses encryption to secure IoT data, reducing breaches and enhancing system resilience • Demonstrating how smart contracts can enforce security policies without the need for third-party involvement	Lack of detailed case studies that demonstrate how blockchain has been successfully applied in real-world IoT scenarios

(Continued)

Table 1 (continued)

Article ref	Year	Blockchain-based features	IoT security	Blockchain-based IoT attacks	Blockchain-based IoT measures	Technical challenges	Future prospective	Main contribution	Limitations
[45]	2024	×	✓	×	✓	✓	✓	• Introduce an approach to the convergence of IoT with machine learning and blockchain • Includes real-world applications of this convergence • Highlights the practical implications of the technology integration	• Evaluating the performance of approaches and algorithms for integrating IoT with ML and BC in various scenarios or applications • Lack of case studies, implementations, and their results in-depth
[46]	2024	×	×	✓	✓	✓	✓	• Examines the security issues that arise when blockchain technology is integrated with Internet of Things systems • Presents a security optimization framework specifically designed for BIoT systems, utilizing threat modeling, machine learning, game theory, and cost analysis to address security vulnerabilities	• Interoperability issues between IoT devices and blockchain platforms are not fully addressed • Ignores social engineering risks and user behavior which affects BIoT security

(Continued)

Table 1 (continued)

Article ref	Year	Blockchain-based features	IoT security	Blockchain-based IoT attacks	Blockchain-based IoT measures	Technical challenges	Future prospective	Main contribution	Limitations
[48]	2022	×	✓	×	×	✓	×	• An examination of current IoT security certifications and their suitability for meeting the demands of diverse IoT environments • Identifying weaknesses in existing certifications and emphasizing the need for security measures tailored to the dynamic and evolving nature of IoT applications	• Most certifications do not adequately assess IoT systems within their dynamic context, focusing primarily on individual devices instead of the entire IoT environment • Existing certifications assess devices based on known vulnerabilities, overlooking unknown or custom software vulnerabilities
This survey	2025	✓	✓	✓	✓	✓	✓	Highlights challenges and issues related to the IoT and blockchain, as well as their integration, which have not been addressed in previous works	While addressing previous limitations, further improvements in scalability/performance/security can be explored in future work

3 Background

To understand how IoT and Blockchain will integrate, it is necessary to have a proper understanding of their background. In this section, we briefly describe the architecture of IoT, applications of IoT, and blockchain technology.

3.1 Architecture of the IoT Network

The architecture of the IoT might be centralized, distributed, or decentralized. As described above, the taxonomy of the main features needed by the Internet-of-Things to support [49] is graphically depicted in Fig. 2.

- **Device heterogeneity:** The IoT includes heterogeneous devices that have different capabilities in terms of computing and communication. This heterogeneity's management must be supported in terms of structure and protocol.
- **Scalability:** Problems with object naming and addressing, communication and data networks, information and knowledge management, and providing and managing services are brought about by connecting objects to the global information infrastructure.
- **Pervasive data interchange via proximity wireless systems:** Wireless communication technologies enable the networking of intelligent objects in the IoT, where the widespread use of wireless media may cause problems in terms of availability.
- **Energy-optimized solutions:** Because IoT devices have limited resources, minimizing energy consumption for communication and computing is a primary requirement. Therefore, optimizing energy consumption is essential.
- **Localization and tracking capabilities:** IoT devices are detectable within the network, and short-range wireless communication facilitates tracking of the whereabouts and motion of intelligent objects. In terms of product life cycle management, this is also crucial.
- **Self-organization capabilities:** Nodes in the IoT organize themselves independently in the network and provide the possibility of sharing data and performing coordinated tasks; in other words, nodes can discover devices and services without the need for another system, build overlap, adaptively adjust the behavior of protocols to adapt to the current network conditions.
- **Semantic interoperability and data management:** The IoT is used to exchange and analyze a massive amount of data. Convert the data into useful information and ensure that the data are presented in appropriate and standard formats for cooperation between different programs.
- **Inbuilt privacy-preserving and security features:** Security should be viewed as a crucial component to ensure privacy and safety in IoT.

Many architectures have been introduced for the Internet of Things, of which there are two famous architectures: three-layer architecture and five-layer architecture. The three-layer architecture is illustrated in Fig. 3a, and the five-layer architecture is shown in Fig. 3b. Gathering information about objects at any time and location is the responsibility of the Perception layer. Transporting object information over the Internet is the responsibility of the network layer. The information gathered must be processed by the application layer [50].

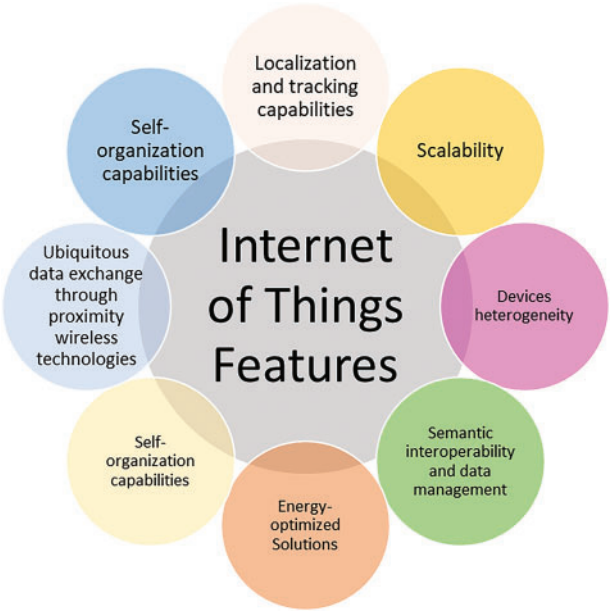

Figure 2: The main features need for the IoT to support

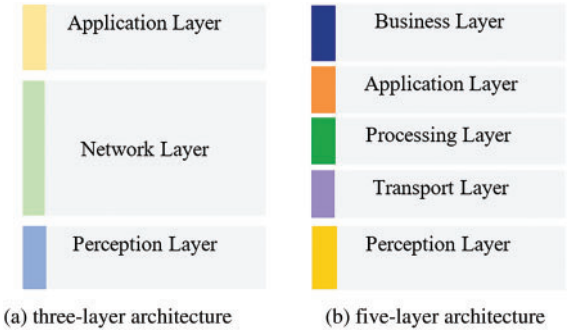

Figure 3: IoT architectures

3.2 IoT Applications

Today, IoT is used in many real-time applications, and numerous fields have developed applications for the IoT. IoT devices can sense and activate via the Internet [51]. IoT applications significantly impact daily life; for example, sensors embedded in the patient's body to monitor the patient's health status, gas leaks in smart homes, smart cities, smart car parking, vehicle location tracking sensory [52,53], smart contracts, wearables [54], automotive [53,55], environment, smart grid, etc. [56,57]. IoT and device-to-device communication [58] are also used in smart retail; in other words, smart retail uses IoT services to increase efficiency and improve performance and inventory system management [59].

3.3 IoT Security

Maintaining privacy in IoT devices is more difficult because they reach the communication and program level later than information gathering. Securing the device to prevent unauthorized users from accessing the data that is stored. The security requirements of any IoT system include confidentiality, integrity, availability, and authentication [60,61]:

- **Confidentiality:** IoT devices gather and handle private user information [62]. Confidentiality guarantees the information's privacy and ensures only authorized users can access and view it [10]. A breach of confidentiality occurs when private information is made public through a data leak.
- **Integrity:** This ensures that an unauthorized person has not changed the information. One of the most common integrity attacks is the man-in-the-middle attack, in which the victim is redirected from a legitimate website to a malicious website. The physical security of IoT devices must be considered to protect them from tampering or unauthorized access, as they are typically deployed in physical environments [63].
- **Availability:** This ensures that the authorized person can access the information at any time [64]. The most significant attacks of this type include DoS attacks, which prevent authorized people from accessing data.
- **Authentication:** Verifies the identity of both sides of communication. Using weak passwords makes it easier for attackers to crack the password [65].

IoT device firmware updates have the potential to introduce vulnerabilities and jeopardize the devices' integrity. As a result, firmware updates should be carefully monitored for vulnerabilities or malicious code [66,67].

3.4 IoT Challenges

The single point of failure is one of the primary issues with centralized IoT network architecture. Additionally, a central server is no longer adequate due to the growing volume of data in IoT networks. Thus, by time-stamping transactions, blockchain addresses these issues in the IoT networks.

The requirement for end-to-end communications in order to carry out automation services was one of the difficulties faced by centralized servers in IoT networks. This issue is resolved by the blockchain's decentralized architecture, which means that IoT devices' autonomy is preserved through its use [68]. By using a decentralized framework that maintains operation even with different levels of device capabilities, blockchain can enhance the management of diverse IoT networks, ensuring that all devices contribute to and benefit from the network.

One of the primary issues with IoT networks is the requirement for an intermediary to handle transactions and information transfers. The blockchain's transparency eliminates the need for a middleman.

Cyberattacks, network issues, and sensor errors can all cause changes in IoT data. IoT data logs and events will be unchangeable once they are stored on the blockchain, allowing for accountability and traceability. Blockchain prevents unwanted changes and uses digital signatures, cryptographic hashes, and decentralized storage to guarantee immutability, transparency, and data security. It guards against data manipulation and cyber threats by offering real-time traceability through audit trails. Consequently, blockchain improves IoT security [69].

Devices with diverse protocols and standards from different manufacturers coexist in heterogeneous IoT environments. Blockchain can offer these devices a common framework for interaction and communication. Creating interfaces that support various device specifications through the use of a modular blockchain architecture enables smooth network integration and communication [70].

Many Internet of Things devices have limited computational and energy resources. Traditional blockchain designs can be resource-intensive, especially those based on proof-of-work (PoW) like Bitcoin and Consortium blockchains. However, blockchain can be made more appropriate for devices with limited resources by modifying its mechanisms, such as with less resource-intensive consensus algorithms like

proof-of-stake (PoS). This modification enables effective transaction processing without taxing the device's capacity. Fig. 4 shows the Internet of Things Challenges.

Figure 4: Internet of things challenges

3.5 Blockchain Technology

Blockchain technology, introduced by S. Nakamoto as the first generation focused on financial transactions, operates as a decentralized ledger where each peer node maintains a shared copy. To create a secure chain of records, the system is organized as a sequence of timestamped blocks, each of which is identified by a cryptographic hash that refers to the hash of its predecessor. Users communicate in a standard blockchain network using private and public keys, signing transactions that are then broadcast to neighboring peers for validation. Predefined rules are used to verify transactions, and if a transaction meets the necessary criteria, it is compiled into blocks that are mined and added to the blockchain [71].

Blockchain databases are dispersed throughout the network rather than kept in one location. A blockchain ledger is a copy of synchronized storage that computing nodes maintain on a broadcast network known as a blockchain network [72]. They use a consensus mechanism to synchronize each node's stored information and generated data [73,74]. Using consensus methods in the blockchain ensures all shared versions are the same. Through the voting of particular nodes, transactions in the consensus mechanism are verified and confirmed quickly [75]. Every subsequent block in a blockchain contains a cryptographic reference to the block before it [76].

The blocks in the blockchain are connected in a chain; therefore, removing and changing one block in the chain also results in changes in the next block [77,78]. Blockchain technology eliminates the need for centralized servers because they are distributed. Decentralized methods, such as blockchain, provide an attractive alternative by establishing a consensus mechanism among several parties, whereas a single point of failure could occur with centralized servers [75].

Blockchain allows people to control how they share their personal data, and they can share it only with the people they want under consented circumstances [58,79–82]. The blockchain's transparency allows users to monitor changes, which deters fraud. As a result, users can be confident that their information is safe [83]. Hashes of the previous and current blocks are included in blocks along with data, as seen in Fig. 4. The

block comprises two sections: the header and the block body. Information about the block is contained in the header. The block was created at the time indicated by the time stamp. Verification is done using the block hash. A set of each block's transactions are stored in the Merkle root. The consensus process produces a number that is known as Nonce. The Nonce is used to solve the proof-of-work algorithm's mathematical puzzle [5].

Accountability and trust among network participants are encouraged by the transparent nature of blockchain, which makes the complete transaction history visible to anybody [84]. Blockchain offers enhanced privacy for data sharing using zero-knowledge proofs. The distributed architecture of blockchain emphasizes elements like user privacy, data consistency, transparency, and resistance to backward changes [85]. State Machine Replication (SMR) is an algorithm blockchain system that guarantees consistency between data replicated on various nodes. Numerous issues with conventional IoT applications are resolved by blockchain. It provides the integrity of IoT data without needing a third party; in other words, blockchain also helps with data protection.

Using blockchain in Internet of Things networks provides a secure and scalable platform for sending sensitive information in a distributed manner. The bandwidth and processing power of the Internet of Things devices are also decreased by blockchain. Blockchain technology is used in various services, such as online micro-payments, supply chain tracking, digital forensics, healthcare record sharing, and insurance payments. Asymmetric cryptography techniques like RSA and ECC, which combine the public and private key, encryption hash, and digital signature generation, are used by blockchain to guarantee the security of user data. As an illustration, consider Bitcoin SHA-256, where the hash function links data blocks in a chain [86]. Fig. 5 shows the structure of blockchain.

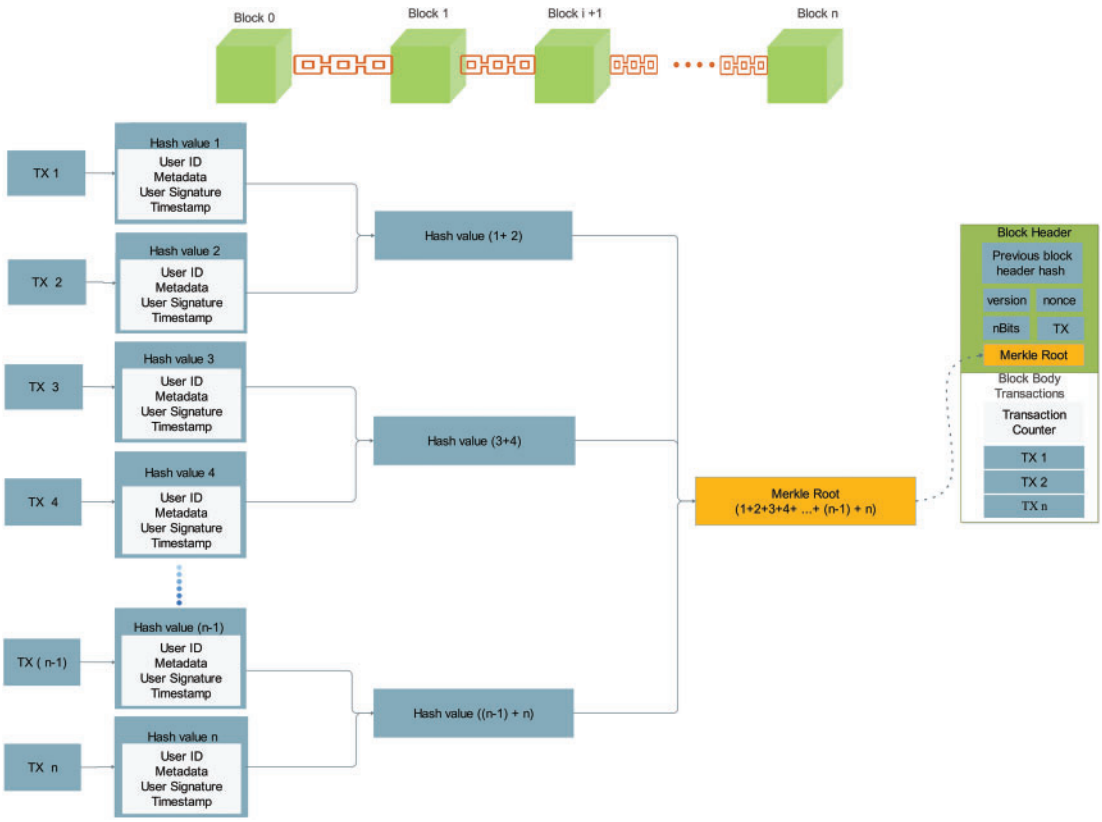

Figure 5: Blockchain strucure

3.5.1 Types of Blockchain Networks

Two perspectives exist for classifying blockchain: the first is based on network type, where there are four types: public, private, consortium, and hybrid; the second is based on the type of blockchain, where there are two types: permissioned and permissionless. Every taut is fully explained below:

Public, Private, Consortium, Hybrid

There are four types of blockchain networks: public, private, consortium, and hybrid [76]. Each node can independently join or leave the network in a public blockchain network. Public blockchains allow any node to join the blockchain network. Examples of public blockchain networks are the Bitcoin and Ethereum networks. A node can only join a private blockchain network with authorization. Access can be authenticated and managed by the network administrator or owner. Only authenticated nodes can participate in the blockchain network [87]. Public blockchains are used in cryptography, whereas private blockchains are used in business applications.

The public blockchain has particular security vulnerabilities. For example, in digital currencies, the hacker attack on the Bitfinex exchange in 2016 led to financial losses of around 65 million US dollars [88]. The cause of this is most likely the infancy blockchain code that hackers use for zero-day attacks. The public blockchain is also subject to the Time Jack attack, in which the attacker manipulates the network's time counter by broadcasting inaccurate timestamps and, in this way, tries to trick the connected nodes into accepting and replacing alternative blocks [89].

Every user on a consortium blockchain network is an employee of its partner companies or the network itself. A hybrid blockchain network effectively combines the features of public and private blockchains while maintaining privacy by allowing nodes to join the network and using the consensus of public nodes to validate transactions that do not contain private data [90]. Hyperledger is an instance of a consortium blockchain wherein a group of peers manages the blockchain. Private and consortium blockchains use Byzantine or benign error-resistant algorithms to control malicious nodes [91]. Table 2 summarizes the key features of blockchain networks.

Table 2: Capabilities of a blockchain network

Capability	Public BCN	Private BCN	Consortium BCN	Hybrid BCN
Decentralization	Yes	Yes	Yes	Yes
Distributed computing	No	No	No	No
Network participation	Open to any node	Approved by network	Approved by network	Depends on different factors
Fault tolerance	Yes	Limited	Limited	Yes
Consensus mechanism	PoW, PoS, etc.	PoW, PoS, etc.	PoW, PoS, etc.	PoW, PoS, etc.

Permissionless and Permissioned Blockchain

Permissioned and permissionless blockchains are the two different types of blockchains [92]. Permissioned blockchains are used in business and institutional procedures, while permissionless blockchains are used in cryptocurrency and financial markets [93]. Permissionless blockchain is maintained and controlled by no one but shared by all network users and updated by miners. Permissionless blockchain systems are public networks that use computing nodes without a priori known identities to manage the blockchain, which can join or leave the blockchain network at any time.

In the beginning, blockchain technology was created as a permissionless system. It was used to host the Bitcoin cryptocurrency, which offered a way for parties to a transaction to stay trusted by acting as a disintermediary. This kind of blockchain relies on the efforts of numerous anonymous miners to solve the hashing of transaction blocks to one another. Trial and error determine how a sophisticated mathematical algorithm competes for that block of transactions. Using a consensus process, other miners confirm the solution once one of them has figured out the algorithm. Through the hashing process and encrypted transactions that guarantee the data's integrity, the authentication of a data block creates a permanent record on the blockchain. Miners can obstruct the process if they work together in concert, but blockchains are generally public and transparent [93].

Permissionless blockchains can only process a certain number of transactions per second. One of the primary concerns with this kind of blockchain is privacy since it could expose distributed ledgers and, consequently, reveal business owners' trade secrets [94].

Permissioned blockchains typically consist of companies that work together to block transactions and have authorized gatekeepers to verify them rather than anonymous miners. 2013 Ethereum and Hyperledger were introduced, two permissioned blockchains [95]. Permission and role must be granted to every node in a permissioned blockchain [96]. Permissioned blockchains offer greater privacy because each member has varying levels of access control.

Permissioned blockchains were undergoing pilot testing by 2016; however, no actual implementation had occurred yet [92]. To increase system performance, permissioned blockchains are needed to parallelize the "execution" stage of various transactions [97]. Permissioned blockchains can be integrated with the Internet of Things to improve efficiency in unmanned aircraft and remote monitoring operations.

All the permissionless blockchain network's nodes maintain copies of the transaction records. Since these copies are continuously synchronized, the data is accurate and up to date, making the network's transactions traceable and visible. They offer total transparency, whereas the permissioned blockchain network allows partial transparency. Some nodes only have a portion of the transaction record copy, and access control settings determine how much information can be accessed. Access control mechanisms prevent unauthorized access to private information [98].

3.5.2 The Blockchain Architecture

Verifier and normal nodes are the two categories of computing nodes found in blockchain networks. Verifier nodes are responsible for verifying transactions because they maintain a replica of the blockchain structure. These nodes also have greater storage and processing capacities than other nodes. On the other hand, normal nodes don't require much processing or storage capacity [90]. They use various communication protocols, such as Kademlia and gossip, to transmit transactions and messages.

Each transaction consists of three parts: data, hash, and hash of the previous block [99]. The five-layer blockchain architecture model is proposed in [90], illustrated in Fig. 6. In blockchain architecture, each layer has its own goal and responsibility.

Each block in the blockchain is uniquely identified by a hash value, with the Genesis block being the first block. The header of each block contains essential information about itself, including the version, root hash of the Merkle tree, timestamp, N-Bits, and Nonce [100].

Similar to the general topology of the network, the blockchain's structure can be divided into three categories: centralized networks, decentralized networks, and hybrid [75,101], as shown in Fig. 6.

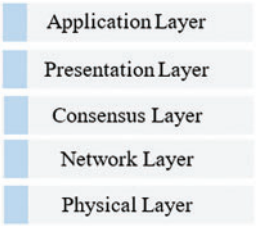

Figure 6: Five-layer blockchain architecture

Centralized: A central node manages all transactions and communication, which has the benefits of faster consensus and simpler efficiency. Communication failures may occur due to this type's centralized data storage structure. The integrity and privacy of the entire network may be in jeopardy if such a central node becomes the primary target of attacks.

Decentralized: Direct communication between network nodes is possible in this centralized or distributed structure. Therefore, a central node is not required to link the nodes. Additionally, transaction processing and data verification are carried out in a distributed fashion within the nodes. Due to the lack of a single point of failure in this network, the data is safer and more reliable. The scalability and consensus speed of this distributed structure are its challenges.

Hybrid: There are multiple central nodes in this type. This design strengthens security and lessens the harm caused by a single point of failure. There may still be problems with centralized control and scalability with this structure. Fig. 7 shows the category of blockchain.

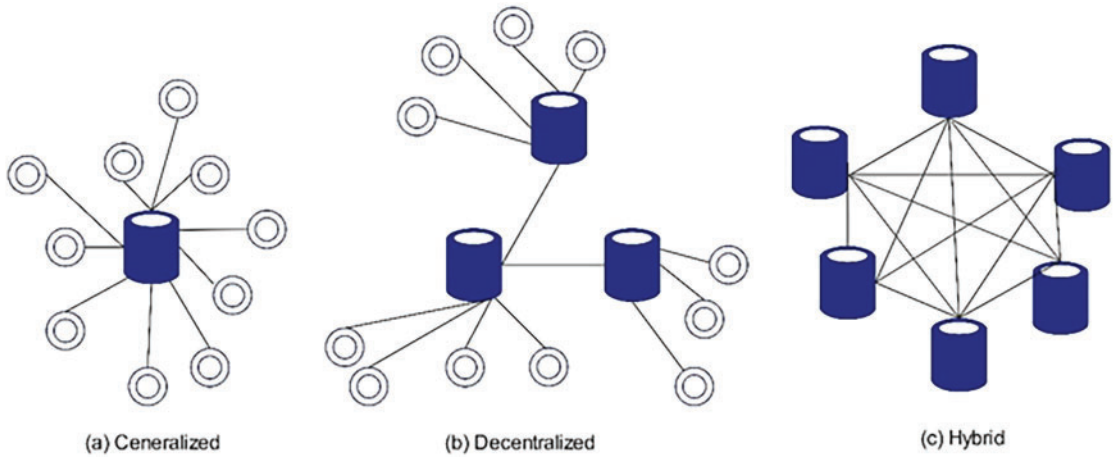

Figure 7: Blockchain network structure categories

3.5.3 Blockchain Features

Decentralization, anonymity, transparency, and immutability are the four primary features of blockchain technology [102,103].

Decentralization: In centralized systems, a third-party agency must verify the authenticity and validity between two nodes, leading to overload. Consensus algorithms are used in blockchain technology, so it has a decentralized structure, and nodes collaborate to maintain the ledger's integrity.

Anonymity: Users can execute their transactions using a randomly generated address because the blockchain lacks a centralized mechanism to track and verify the legitimacy of the addresses.

Immutability: The blockchain guarantees data integrity, as once a transaction is entered into the system, it cannot be modified or removed. When someone tries to alter information in a blockchain block, the hash correspondingly modifies, indicating an attempt to alter blockchain data.

Transparency: Blockchain makes transactions publicly visible and allows all nodes to track and audit historical records [104].

Cryptographic: A pair of private and public keys is used to encrypt transactions stored on the blockchain. The data is broadcast over the network after encryption with the sender's private key [94].

3.5.4 Blockchain Challenges

Although blockchain has many advantages, this section describes the challenges in blockchain:

Scalability: Scalability is one of the primary issues with blockchain. Existing blockchain architectures handle large numbers of transactions, which can cause network congestion and raise transaction costs. To improve scalability, increasing throughput and decreasing congestion can ensure smoother operations on blockchain networks [105].

Storage capacity: Because the network exchanges and processes more messages, scalability problems associated with increasing the number of copies have a detrimental effect on network performance metrics like throughput and delay [106].

Security: As its decentralized nature, blockchain does not ensure security. Misconfigurations, coding mistakes, and other defects could happen. Solutions like formal verification methods, secure coding practices, and frequent security audits must address these vulnerabilities [107].

Anonymity and data privacy: Blockchain allows devices to interact with each other without the involvement of servers. Due to the public key's visibility to other network peers, blockchain may be susceptible to breaches in transactional privacy [108].

Smart contracts: A collection of data and codes maintained at a particular blockchain address is called a contract. Devices may use a contract's public functions. Functions can start events. The application logic of IoT applications can be safely modeled by smart contracts [109]. Ensuring smart contracts are secure and reliable is essential to preserving the integrity and trustworthiness of the blockchain system [46].

Legal issues: The IoT space is influenced by a country's privacy laws or regulations. Revisions to most of these laws are necessary, particularly considering the introduction of blockchain technology. Developing new rules and regulations will help facilitate the certification of security features, making the IoT network more secure and reliable.

Consensus: IoT devices are inappropriate for consensus mechanisms because of resource constraints. The blockchain network's consensus protocol determines how many resources are needed. Tasks are usually assigned to unrestricted gateways or processors by solutions. Another suggestion for this problem is to use off-chain solutions to reduce the delay in the blockchain.

3.5.5 Blockchain Applications

Blockchain is used in various fields. Traditional industries may apply blockchain technology to improve system efficiency [110]. In this section, examples of blockchain applications in the real world are described [111].

Cryptocurrencies: Blockchain technology is used by cryptocurrencies such as Bitcoin and Ethereum to facilitate safe and transparent transactions. Transactions are now peer-to-peer since blockchain technology and related protocols are decentralized, eliminating the need for intermediaries such as banks. Because this technology disrupted the established financial system, it garnered much attention.

Supply Chain Management: Blockchain technology improves the traceability and transparency of financial transactions in supply chain management. Blockchain assures authenticity by tracking the product's location in an unchangeable ledger at every stage, lowering the possibility of fraud and imitating it to defraud [112]. It allows consumers and businesses to verify the origin and quality of goods.

Financial Services: Blockchain can completely transform the financial services sector because of its features, which include being more secure, faster, and affordable. It eliminates the need for an intermediary, speeds up transaction settlement, and eliminates transaction fees [113]. Blockchain-based systems streamline payment procedures and enhance identity verification.

Healthcare: Decentralized access and secure patient record storage are made possible by the application of blockchain technology in the healthcare industry. Blockchain protects sensitive medical data and allows for private, secure access. In Addition, it guarantees the confidentiality of patient data [114]. Moreover, blockchain makes drug supply easier. Blockchain is being used by many organizations to distribute and safeguard health data, providing insurers with high-quality information while cutting down on administrative expenses [115].

Voting Systems: Voting systems based on blockchain technology offer more excellent reliability because each vote is transparent and verifiable. Because this system keeps votes in a decentralized ledger, data cannot be manipulated, making voting transparent and verifiable and lowering the possibility of vote fraud and forgery.

Intellectual Property Protection: Blockchain technology creates a decentralized, transparent ledger, which also aids in the protection of intellectual property. Blockchain technology aids in the prevention of unauthorized resource use and plagiarism. Blockchain facilitates equitable compensation for the inventiveness of creators.

Real Estate: Blockchain technology can make real estate transactions easier and offers solutions in this area. Transparency and safety are enhanced by smart contracts [116], which eliminate the need for intermediaries in the transfer of property ownership. Providing confidential property history records achieves increased trust and decreased real estate market fraud.

Energy Sector: Blockchain makes it possible to trade energy as the globe shifts to renewable energy. Renewable energy can be produced by individuals using decentralized energy and sold via a blockchain platform. Assists in creating a cleaner and more efficient energy ecosystem.

Supply Chain Financing: By confirming the transaction data stored in the blockchain, lenders can lower risks and offer financing options to companies facing financial difficulties. Consequently, they can grow businesses and strengthen the supply chain network.

Identity Management: Identity management systems are also advanced by blockchain technology. The architecture of blockchain technology facilitates identity management by granting rights to people with greater control and protection of personal data. Blockchain reduces the risk of data breaches and makes an individual's identity unforgeable by enabling decentralized storage and selective sharing of identity information. Blockchain technology has been used by some airlines to manage flight information and to create a billing system that authenticates passenger identities [117]. Below, Fig. 8 shows the applications of blockchain.

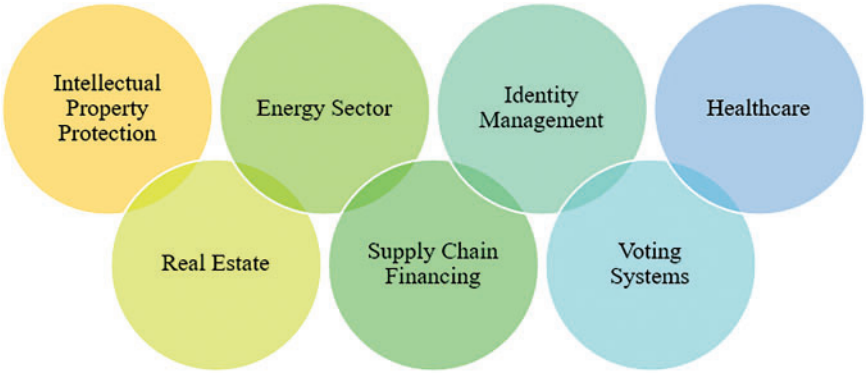

Figure 8: Applications of blockchain

4 IoT and Blockchain Integration

Blockchain is a DLT that securely stores and transmits data agreed upon by all mining nodes in an encrypted and authenticated manner. These data are secure and immutable [7]. The immutability of blockchain technology presents an opportunity to improve IoT authentication [118]. The Internet of Things network's nodes may not currently trust one another, but blockchain can help to establish trust [119]. Blockchain blocks that use timestamps are connected to one another through cryptographic hashes [120]. The integration of blockchain technology and the Internet of Things has been predicted to be one of the most critical factors in creating a revolution in digital transformation in various fields [49]. IoT security gaps can be filled with fundamental blockchain network characteristics such as transparency, verifiability, data redundancy, and reliability [90,121]. Real-time transaction visibility via the distributed ledger is made possible by the combination of blockchain technology and the Internet of Things [122].

Interoperability, resource constraints, and vulnerabilities are some of the significant issues facing the Internet of Things. Using blockchain technology can help to improve the confidentiality, integrity, and availability of data in IoT networks [10]. The Internet of Things (IoT) has much to gain from the blockchain's functionality and can help advance existing IoT technologies. Blockchain's decentralization, consensus process, data encryption, and smart contract features make it a good choice for guarding against possible intrusions in the Internet of Things network [47]. Public key cryptography can be used by blockchain technology to confirm that Internet of Things transactions and blocks are legitimate before appending them to the chain [123].

The integration of the Internet of Things and Blockchain is a noteworthy development in the computational communication system. Blockchain can assist with important IoT security needs [21]. There are no trust mechanisms between IoT devices, which create security problems. Blockchain uses consensus mechanisms to provide Internet of Things security [124]. This integration would be a significant revolution in situations where many participants need to exchange IoT information securely.

New opportunities, such as incentive strategies, are created by integrating blockchain technology with IoT networks and using tokens and smart contracts in these networks.

In practice, blockchain enhances IoT across a range of sectors. It offers real-time shipment tracking and verification in supply chain management, which lowers fraud and inefficiencies. In smart cities, blockchain secures data from connected infrastructure like traffic sensors and energy grids, ensuring reliability. Blockchain technology protects patient data on healthcare IoT devices, allowing for private and secure provider sharing.

Smart contracts on the blockchain also eliminate the need for middlemen by automating transactions between IoT devices. To ensure effective energy distribution, smart meters, for instance, can independently purchase and sell electricity in response to real-time demand. In addition to promoting data sharing in IoT networks, token-based incentive models also help industries like manufacturing's predictive maintenance.

Blockchain integration improves the security, transparency, and efficiency of IoT ecosystems while accelerating digital transformation in a number of fields.

Real-World Applications and Case Studies

- The integration of IoT sensors with blockchain helps to increase the security and transparency of supply chain operations. IoT sensors monitor parameters such as temperature, humidity, and location. Then, this data collected from sensors is stored on the blockchain, and as a result, a tamper-proof and audible record is provided.
- Secure access control is facilitated by blockchain technology in smart home systems. The blockchain provides a unique identity for every device, which is utilized for authorization and authentication procedures.
- Integrating blockchain technology with IoT devices creates a decentralized healthcare data management system. Medical devices with IoT capabilities gather patient data and securely store it on blockchains. Blockchain and IoT integration can improve patient data management by protecting privacy and data integrity. Attribute-based encryption (ABE) and homomorphic encryption are two examples of advanced cryptographic techniques that enable safe data operations while protecting patient privacy. Ensuring that sensitive patient information is accessible only to authorized medical personnel is imperative [125,126].
- Blockchain and Internet of Things integration can increase compliance in the nuclear energy industry. Blockchain technology guarantees that all regulatory data is recorded transparently and securely, enhancing regulatory supervision and auditability.
- Blockchain technology combined with the Internet of Things can optimize energy consumption and distribution in the energy sector. Blockchain technology can protect the real-time data collection capabilities of Internet of Things devices, guaranteeing that the data is reliable and unchangeable. This may result in increased effectiveness and a decrease in energy transaction fraud [126].
- Blockchain technology can improve the use of IoT in smart cities by securing data from various applications, including public safety, environmental monitoring, and traffic management. It guarantees the security and reliability of the sensor data collected.
- The benefits of integrating blockchain and the Internet of Things include improving security and privacy, increasing speed, reducing costs, improving reliability, and eliminating a single point of failure [38]. Several blockchain IoT projects, such as IoTA, Waltonchain, IoTex, Ambrosus, Moeco, and Atanomi, have impacted the business and industry. In addition, there are some real blockchain-based IoT examples, such as Telstra, Mediledger, NetObjex, and Slock. It, and Drone on the Volga [28].

Although there are many advantages to integrating blockchain and the Internet of Things, there are also obstacles in the real world. The inherent limitations of IoT devices cause these obstacles. Limitations include task distribution, energy consumption, and the computing power of IoT devices. It should be noted that there have been studies in this area in recent years [127–129].

A key aspect of using blockchains in the IoT is using cryptographically impenetrable databases as connection nodes [60]. Blockchain can help in the more efficient use of computing resources, storage capacity, and broadband of distributed idle IoT devices, thus reducing costs [130]. Some improvements that this integration can bring include:

- **On centralization and scalability:** Integrating IoT and blockchain can improve the system's fault tolerance and scalability; additionally, it helps improve IoT scalability.
- **Identity:** Blockchain technology can provide reliable distributed device authorization and authentication for Internet of Things applications [131].
- **Autonomy:** Next-generation application features and the creation of intelligent autonomous assets and hardware as a service are made possible by blockchain technology.
- **Reliability:** Blockchain technology allows for the distribution of IoT data over time while maintaining its immutability. System users are guaranteed that the data are authentic and have not been altered by their ability to confirm this.
- **Security:** Transactions on the blockchain allow secure storage of communications and information. Blockchain technology can be used to optimize the secure standard protocols currently used in the Internet of Things [132].

The location of these interactions must be determined when integrating blockchain: through blockchain, inside the IoTs, or in a hybrid design combining the two [133]. This article [98] introduced a blockchain-based trust architecture to build end-to-end trust for IoT-based applications. In this article, they proposed [134] an access control scheme based on attributes and collaboration on top of a blockchain for IoT devices. This article introduces a distributed blockchain system to ensure and detect the integrity of IoT data [135].

According to forecasts, the top 5 integrations of blockchain and IoT by 2030 will be e-government, digital economy, self-sovereign identity standard [136], global supply chain management, and digital energy and smart grid [137], as shown in Fig. 9. Blockchain can be critical in IoT systems' authentication and authorization management. Block stack [138] is a common blockchain technique that uses JSON web tokens to authenticate IoT transactions.

Figure 9: Top 5 blockchain and IoT integration predictions by 2030

By providing a distinct GUID and PKI pair to every IoT device, blockchain can enhance key management among IoT devices. Therefore, blockchain effectively reduces runtime computation and memory management needs in secure communication between IoT devices [132]. For the messaging protocol, the integration of blockchain protocols into the IoT communication layer is proposed [139], as well as the use of TeleHash based on Kademlia DHT [140]. TeleHash [141] is a lightweight and secure protocol for P2P communication that uses encryption for secure mesh communication.

In [142], the authors introduced a blockchain-based framework to solve the security problem of sharing lightweight information on the Internet of Things. This framework provides a double-chain model combining blockchain data and transactions. Blockchain data are responsible for the distribution of storage and data integrity. The transaction blockchain is also responsible for data registration and resource and data transactions.

In [143], the authors presented a firmware management architecture using the Interplanetary File System (IPFS) and blockchain technology. By guaranteeing reliability, blockchain technology enhances data integrity and offers a distributed database. Researchers have developed a blockchain-based Internet of Things data-sharing framework to manage and store edge resource allocation [144]. Fig. 10 shows the applications of BIoT.

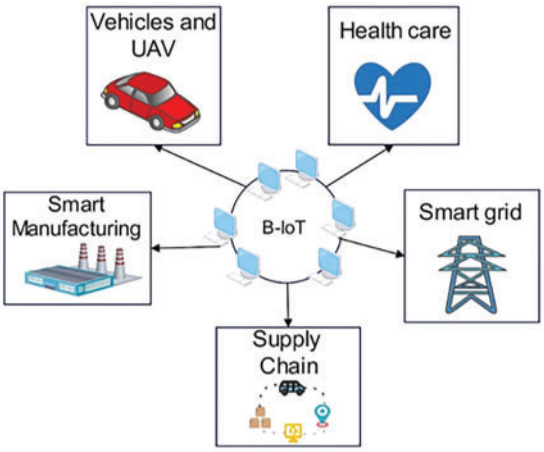

Figure 10: Applications of BIoT

This paper [12] introduces a new method integrating FL, dense neural networks, and blockchain technology to improve Internet of Things security protocols. This method utilizes the security features of blockchain for privacy and data integrity. Through a quantitative approach and experimental validation of the Internet of Things's real data, it has introduced new security efficiency measures and comparative improvement factors. The advantage of this method is that it increases the integrity of the data and the learning model. However, this method has limitations in terms of compatibility with various Internet of Things devices and diverse environments.

This paper [145] presents a PUF-based device authentication model integrated with blockchain technology's "Energy Proof" consensus algorithm to improve the security, effectiveness, and scalability of Internet networks for medical equipment. A layer of defense against impersonation and the creation of false data is created by using PUF keys to generate the device's identity. This approach has the benefit of lowering energy and storage overhead while simultaneously accelerating transaction processing and enhancing system security. This article [146] proposes a blockchain-based reputation assessment system to identify malicious devices that aim to cause harm in IoT networks. The system determines a device's reputation value by calculating its communication time, quality, and historical reputation value. As a result, it guarantees the device communication's security. When malicious behavior is noticed, this suggested scheme will quickly lower the reputation score of the device.

Blockchain-based IoT access control solutions are becoming increasingly popular [147]. The system decentralizes access control decisions by leveraging attribute-based access control models and identity-based signatures, ensuring verifiability and immutability. The system enhances security by preventing DDoS attacks, facilitating secure cross-domain access, and providing efficient access control mechanisms. By incorporating security features and design considerations, the Blockchain-Based IoT Access Control System significantly enhances IoT security by providing robust access control mechanisms, resilience against attacks, and efficient cross-domain access management. Scalability challenges may arise as the number of devices and transactions increases. The article does not extensively address how the system handles scalability issues

in large-scale IoT deployments. In [148], the SDACS framework for IoT networks is introduced, integrating attribute-based access control, hyperledger fabric blockchain technology, and interplanetary file system. This schema can solve the key challenges in IoT data sharing and address privacy concerns, data security, and scalability issues.

An architecture was suggested to improve the security of machine learning models in IoT networks. The introduced model [149] enhances overall security and trustworthiness in IoT networks by combining deep learning, edge intelligence, and blockchain technology to provide a reliable and secure solution for managing data exchange and access control. Integrating blockchain technology with deep learning models for edge intelligence in IoT networks can introduce complexity in implementation and maintenance, which may pose challenges for adoption and scalability. IoT environments with limited resources may find it difficult to implement blockchain-assisted solutions due to the potential need for large computational and energy consumption. This paper [135] introduces a distributed blockchain data simulation system for IIoT applications to detect and guarantee data integrity. Maintaining the integrity of IoT data is challenging, but it is an essential component of data flow. The elements of the suggested system are data generation, data storage in a database built on the blockchain, and data reading stored in the blockchain. Reliability and accuracy of the data are also impacted when data integrity is violated.

This paper [97] presents a layered architecture to enhance end-to-end communication in blockchain-based Internet of Things applications. The blockchain layer's trust evaluation modules verify the block's integrity, while the data layer assesses the sensor's dependability. The blockchain can help establish trust on the Internet of Things, where nodes do not trust one another. Sensor nodes use information from other node observations to create a reputation history that considers the node's long-term behavior. The likelihood of an attack on a node decreases with increasing reputation value. This paper [150] focuses on the feasibility of using blockchain technology to address the trust issue in Internet of Things applications. Thus, the IoT database's availability is restricted to establish trust. This blockchain-based secure data-sharing model aims to monitor data integrity across various IoT systems. Its novelty lies in integrating a lightweight consensus mechanism and using smart contracts to ensure data integrity and traceability. While the method aims to be lightweight, blockchain integration still requires significant computational power, which may not be feasible for all IoT devices, especially those with limited resources.

This paper [151] presents a blockchain-based trust-enabled CDP system with reinforcement learning to give the Internet of Things network a safe and reliable business environment. Smart devices in IoT networks receive data in real time, enabling the rapid development of Crowdsourced Data Trading (CDT) systems. A blockchain-based two-way smart contract is also introduced to establish a trade-off between cost and benefit within a safe system via the Internet of Things network. It also suggests a traceable trust computing (TTC) scheme to filter malicious devices further and enhance system security. This scheme performs previous trust evaluations based on historical data backtracking to correct previous trust evaluations.

Data privacy is still a major concern, even though blockchain integration with IoT improves the security of IoT data. This paper [152] presents a blockchain-based architecture that implements various privacy at the data stream level produced by IoT devices by applying Laplace noise and Gaussian noise using a low-complexity cryptography mechanism and a fast convergence protocol to preserve privacy in blockchain-based IoT networks. The owner can designate three levels of privacy in this DP-based architecture: low, medium, and high. This paper [153] presents an encryption architecture based on decentralized hierarchical attributes. This suggested architecture combines blockchain technology with edge computing to enable safe information sharing across various networks. Protecting user privacy is the goal of this IIoT architecture. This architecture also uses decentralized authentication. Implementing this architecture reduces the risk of

unauthorized access because only a user whose identity has been confirmed can decrypt the data and access sensitive information based on their attributes.

This paper [154] presents a deep learning-based blockchain architecture designed to protect the privacy and security of transmitted data for the security of industrial IoT networks because there is a chance that hackers could engage in malicious activity between entities when data is transmitted over an insecure communication channel. Additionally, a unique key is generated for every device using a secure hash algorithm. A deep neural network algorithm is created to carry out the encryption and decryption procedure for every data record. Information that has been encrypted is kept in separate blocks. It optimizes the validation process and guarantees effective and secure communication between devices by capturing contextual information from both historical and future data using an Enhanced Bidirectional Long Short-Term Memory (EBLSTM) algorithm. This paper [155] presents a two-level blockchain-based IoT privacy protection framework incorporating deep learning methods. MABLSTM is used to authenticate the user and the collected data, which is the first level of privacy. After authentication, the data is saved in the blockchain database. The second level of privacy encrypts the data using Elliptic Curve Cryptography (ECC) and the encoder portion of Autoencoder.

In [156], the authors introduced a framework for decentralized data transmission in IoT networks that integrates blockchain and SAGIN to secure data transmission within the network, making it impossible for hackers to access and alter the data. The suggested framework uses distributed consensus and asymmetric encryption features to improve security. This paper [157] presents BlockRep, a blockchain-based reputation system for the Internet of Things (IIoT) retail sector that guards against Sybil attacks like competitors injecting false negative reviews and retailers injecting false positive reviews. Therefore, the authentication process is based on the accuracy of cryptographic tokens. The legitimacy of retailers' reputations is guaranteed by this approach, which also removes the need to trust e-retail platforms and ensures the anonymity and authenticity of reputation systems. In [158], the authors presented BBAD, a blockchain-based assured deletion scheme for Internet of Things networks that employs MHT for public deletion verification, Shamir secret sharing and re-encryption for secure key deletion, and smart contracts for access control during the data validity period. Additionally, after deletion, it allows public verification, so a reliable third party is not required.

In [159], the authors proposed a blockchain-based decentralized dual identity management and authentication framework to enhance IoT network devices' security and management. Every IoT node in this newly introduced framework is given a dual identity, which makes the secure authentication process easier. The framework provides IoT devices with two identities: blockchain-generated and device-inherited identities. This dual strategy improves the network's security and traceability of device interactions. Table 3 summaries these recent methods of integrating Blockchain for IoT.

Table 3: Summary of recent frameworks integrating blockchain and IoT

Ref.	Criteria	Method	Advantages	Limitations
[134]	Authorization	To ensure the security of real-time IoT authorization, the Attribute-Based Access Control method leverages blockchain technology to enhance access control technology in the Internet of Things	• Enhanced Security • Efficiency • Scalability	• The complexity of Implementing and managing • Privacy concerns related to storing sensitive access information on a public ledger

(Continued)

Table 3 (continued)

Ref.	Criteria	Method	Advantages	Limitations
[135]	Integrity	The Data Integrity Detection Model uses blockchain technology to guarantee data integrity in Industrial Internet of Things (IIoT) applications	• Quickly identify unauthorized changes • Enhancing trust in the data stored	• Data length restrictions may limit the kinds of data that can be processed and stored on the blockchain in an efficient manner, which could affect the modularity of the system • The system may involve significant costs • Significant computing resources, which could be a limitation for organizations with limited IT infrastructure
[12]	Integrity	This research advances IoT security by including LR and DNNs in the FL configuration and utilizing blockchain technology.	Improves the training of models and data integrity	Having limited adaptability with a wide range of devices and Internet of Things environments
[145]	Authentication	Combining blockchain technology with Physical Unclonable Function (PUF) to guarantee safe IoMD device authentication	• Lowering energy and storage overhead • Improving transaction processing speed and overall system security	Insufficient standardization for real-world implementation
[154]	Authentication	Integrates deep learning with a blockchain framework to enhance security in Industrial Internet of Things (IIoT) networks	Improving authentication accuracy and reducing processing time for data transactions	• Dependency on trusted authority • Implementation complexity • Computational overhead
[155]	Authentication	Combines Long Short-Term Memory (LSTM) and Adaboost for authentication and utilizes an autoencoder with ECC-based data encryption	Enhance accuracy and precisionion	Adaptability of the framework to various IoT applications and environments
[159]	Authentication	Utilize the benefits of blockchain technology to offer a strong identity management and authentication solution for IoT networks	Enhance security, traceability, and accountability	The implementation of dual identities and secure data uploads may impose resource overhead
[148]	Encryption	Punishment mechanism for malicious users and the encryption of data stored in IPFS	Enhance the security and privacy of IoT data sharing	Lack of real-world implementation and validation of the schema
[147]	Access Control	Implementation of a blockchain-based IoT access control system	• Robust access control mechanisms • ResIlience against attacks	• Scalability issues • Integration complexity
[149]	Access Control	Method for integrating deep learning models and blockchain technology to improve data processing, security, and efficiency in Internet of Things networks.	• Decentralized access control • Enhanced security	• Resource requirements • Scalability issues • Complexity

(Continued)

Table 3 (continued)

Ref.	Criteria	Method	Advantages	Limitations
[158]	Access Control	A blockchain-based scheme that uses Shamir secret sharing to safely handle keys and ciphertext while letting data owners establish their deletion time limits. It also includes a public verification system that allows confirmation of deletions even when the data owner is not online.	• Enhancing security • Elimination of the need for a trusted third-party • Reduces the risk of a single point of failure • Low computation	Energy consumption and scalability
[119]	Trust	A lightweight block generation mechanism where gateway nodes send blocks to other blockchain nodes for validation	Improving block validity with the help of trust management	• Scalability of the trust calculation process • Resource utilization
[150]	Trust	Blockchain-based secure data-sharing system lies in integrating a consensus mechanism and using smart contracts to ensure data integrity and traceability.	Enhances security	• Computational Overhead • Complexity of Implementation
[151]	Trust	Create a secure and efficient environment for data trading by integrating blockchain and reinforcement learning methods to enhance data accuracy and trustworthiness in the IoT ecosystem.	Improves data quality and security	• Dependence on Historical Data • Resource Intensive • Regulatory and Privacy Concerns
[156]	Trust	Blockchain-based data security transmission mechanism for securing communication of IoT devices	• High throughput • Low latency • Enhance security	• Complexity of Implementation • Dependence on Network Conditions
[157]	Trust	A blockchain-enabled reputation system designed for the IIoT-enabled retail industry. This system utilizes tax-endorsed reviews to ensure that any malicious retailer attempting to post fake reviews incurs additional tax fees	Enhancing the authenticity of retailer reputations resilience against Sybil attacks	Complexities and challenges of integrating the proposed system into existing e-retail platforms
[152]	Privacy	Method, which integrates differential privacy techniques with a blockchain framework, allowing IoT data owners to set customizable privacy levels	Ensuring secure data tranmission continuous auditing for privacy compliance	• Increased processing overhead storage demands • Potential for Data Inaccuracy
[153]	Privacy	Lightweight authentication and data encryption based on user attributes, enabling efficient and privacy-aware data transactions between IoT devices and cloud servers	Improve security and trust	Scalability issues

5 Challenges of IoT, Blockchain, and Integration

Deploying IoT applications on blockchain systems is still challenging. The architecture of an IoT blockchain system needs to support many IoT devices. Second, because IoT devices have limited storage and

processing power, the consensus mechanism in the blockchain, which maintains peers' data integrity needs to be specially created for IoT blockchains. Third, to achieve high system performance in IoT blockchains, traffic modeling of a blockchain network is necessary. A thorough understanding of a traffic model can improve communication processes and protocols.

- **Storage capacity and scalability:** In IoT, devices can generate gigabytes of data in real-time, which is a major obstacle to blockchain integration of the IoT, as a small number of transactions can be processed per second by certain existing blockchain implementations. It might act as an IoT bottleneck. In other words, the IoT consists of thousands of heterogeneous devices continuously generating large amounts of data. Scaling blockchain in IoT networks is a big challenge because the blockchain isn't meant to store much data [132].
- **Resource constraints:** IoT devices have limited resources, while blockchain requires much processing power, bandwidth, and speed [160,161]. For instance, the main consensus mechanism in most blockchain systems is proof-of-work. However, proof of work requires significant computing power. One of the main resource limitations of IoT devices is energy limitation. Therefore, energy efficiency is one of the main aspects of long-term computing maintenance of IoT nodes. Blockchain mining [162] and P2P communication [163] cause nodes to consume energy. Proof-of-stake [164] and proof-of-space [165] algorithms are suitable for mining processes. Mini-blockchain [166] is also ideal for P2P communication to reduce energy consumption. Encryption techniques such as Myriad or Scrypt [167] and multi-algorithm mining are faster than other algorithms and can significantly reduce energy consumption [100].
  - **Security:** Internet-of-Things applications face security issues at various levels due to inefficiency and high device heterogeneity. The characteristics of the Internet of Things, such as mobility, wireless communication, and scaling, affect security [168–170]. IoT and blockchain integration can also impact IoT communications [132]. Slock proposed a blockchain framework for security, identity, coordination, and privacy challenges for IoT devices.
  - **Anonymity and data privacy:** Because IoT applications deal with confidential data, privacy and anonymity are essential. Blockchain is the best solution for identity management on the Internet of Things. For instance, blockchain technology is used in BIoT healthcare applications to store patient health data, and the patient's identity must remain confidential [171].
  - **Absence of an IoT-focused consensus mechanism:** Most real-time IoT systems need instantaneous. Transaction confirmation shouldn't use consensus finality since it causes a delay in Transaction confirmation. PoET also requires special hardware, which is why it is not suitable for Internet networks. Current consensus protocols such as PoW, PoS, PoET, and IOTA are designed for permissionless blockchains. However, PoS and PoET can also be applied to permissioned blockchains [172]. The primary problem with these consensus protocols is that they are susceptible to blockchain forks because no permanently committed block is produced by the consensus process, which is probabilistic in nature [49]. It is possible to increase performance and decrease power consumption by eliminating the BC Proof of Work (PoW) consensus mechanism [173]. Conversely, Proof of Work (PoW) guards malicious Sybil attacks and ensures that Blocks cannot be altered. Therefore, the objective is to improve BC procedures to align security and efficiency properly [143].

Blockchains have integrated consensus mechanisms as fault-tolerant systems for verifying transactions, with these mechanisms serving as a means to maintain agreement among network nodes. However, as the network expands and the number of nodes increases, achieving agreement becomes more challenging. In public blockchains, user participation is essential for verifying and authenticating transactions. Due to the dynamic and self-regulating nature of blockchain, it necessitates the incorporation of a secure mechanism to confirm the authenticity of transactions, enabling participants to reach a consensus. Several consensus

mechanisms have been proposed, each with unique fundamental principles and applications. PoS, the most well-known substitute for the PoW mechanism, selects validators for new block creation at random. A node's chances of being chosen to validate the following block are based on how many assets or stakes it has. In contrast to PoW, which necessitates expensive mining techniques because of its high energy consumption, PoS is made to remove challenging computational puzzles, which lowers mining costs [71].

It is possible to determine which node has the authority to publish the next block using consensus models like "proof of work" and "proof of authority". Through a consensus mechanism, participants agree to transactions and records, making certain that every party's perspective of the shared database is in line with everyone else's. This removes the need to have faith in other participants, who might act maliciously or with different intentions. Any improper modification or tampering of the data will be independently detected and rejected by honest participants through the consensus mechanism. Therefore, once they are stored on the blockchain or transferred, digital assets and records cannot be altered without the participants' approval in the form of a digital signature [70].

A consensus algorithm called PoA has been suggested for permissioned blockchains. The PoA algorithm is implemented in two ways: Clique and Aura. Although they both employ a similar block proposal scheme, Clique does not need a block acceptance procedure. After a majority of authorized entities have signed it, each proposed block is approved. The PoA consensus's primary benefit is the ability to execute more transactions simultaneously and it requires fewer computational resources [174].

As more users join the network, the scalability issues with blockchain could become a major concern that worsens over time. However, these issues can be minimized to a manageable level by employing the appropriate consensus algorithms. PoW is unsuitable for an IoT environment due to its massive power consumption [175]. Table 4 shows a comparison of blockchain consensus mechanisms.

Table 4: Comparison of blockchain consensus mechanisms

Consensus mechanism	Type of consensus	Permission type	Scalability	Security	Latency	Energy consumption	Suitable for IoT?
PoW	Competitive	Permissionless	Low	Very high	High	Very high	No (High resource demand)
PoS	Competitive	Permissionless	High	High	Medium	Low	Partially (Requires strong validator nodes)
PoA	Collaborative	Permissioned	High	Very high	Very low	Very low	Yes (Low energy, fast transactions)

Challenges of integrating blockchain in IoT applications

The tradeoff between power consumption, performance, and security: Implementing blockchain algorithms requires considerable computing power, which is challenging for IoT devices with limited resources. The solution to this challenge proposed by the researchers is to optimize the central algorithms to increase the number of approved blocks per second. For example, although removing the blockchain proof-of-work consensus mechanism improves efficiency and reduces energy consumption [173], the disadvantage of this

solution is that the network becomes vulnerable to malicious Sybil attacks. Therefore, the aim is to balance security and efficiency well [176].

The tradeoff between concurrency and throughput: The constant data flow from IoT devices leads to high concurrency [177]. Because blockchain throughput is limited, quickly synchronizing new blocks between blockchain nodes in a chain structure ledger requires a lot of bandwidth to improve throughput [178]. Therefore, increasing blockchain throughput on the Internet of Things network is challenging.

The tradeoff between transparency and privacy: Blockchain can ensure transaction transparency by maintaining an immutable record of every transaction [179], which conflicts with privacy. Therefore, it is necessary to maintain a balance between transparency and privacy to control access to IoT using blockchain. Creating an affordable access control system for IoT using blockchain is required to preserve a balance between privacy and transparency.

Handling big data on the blockchain: The need to manage large amounts of IoT data on the blockchain poses a challenge in integrating blockchain and IoT applications due to the limited storage capacity of devices. Studies conducted in 2018 showed that with 1000 participants and each participant exchanging a 2 MB image in the blockchain application every day, each blockchain node requires 730 GB of storage space in a year. Therefore, the challenge is that more blockchain storage space is needed [180].

Regulatory problem in BC technology: Although blockchain's features of decentralization, automation, immutability, and anonymity have brought many benefits to IoT applications, they also bring new regulatory challenges [181]. One of the challenges that blockchain automation poses is errors in the code, the consequences of which are the loss of data or the execution of unauthorized transactions. Intentionally obfuscating or hiding the code also hinders understanding the purpose of the smart contract or code. If a malicious agent executes the smart contract, it can harm the network or its users [41]. The current rules and regulations of the IoT are becoming outdated with the emergence of new technologies such as blockchain, as these rules were designed for a centralized world and do not consider the DTL feature. Due to the immutability of blockchain, the data generated in DTL is permanent and cannot be changed or deleted. Additionally, there is no central control over records before publication; therefore, they can't be filtered or removed in privacy-violating circumstances. Hence, sensitive information can be published without the need for authorization or vetting. A lack of governance leads to problems in identifying parties involved in illegal activities. In other words, tracing the source of illegal activities, such as money laundering or fraud, has become challenging.

Connection problem with IoT devices: IoT devices generate large amounts of data that must be processed, stored, and analyzed. Therefore, IoT devices are expected to be connected to high computing storage and network resources to exchange data. High computing storage space enables efficient data management. However, the Internet of Things has limited capacity to connect to blockchain technology. Fig. 11 illustrates the challenges of integrating blockchain into IoT applications, while Table 5 summarizes the solutions to these challenges.

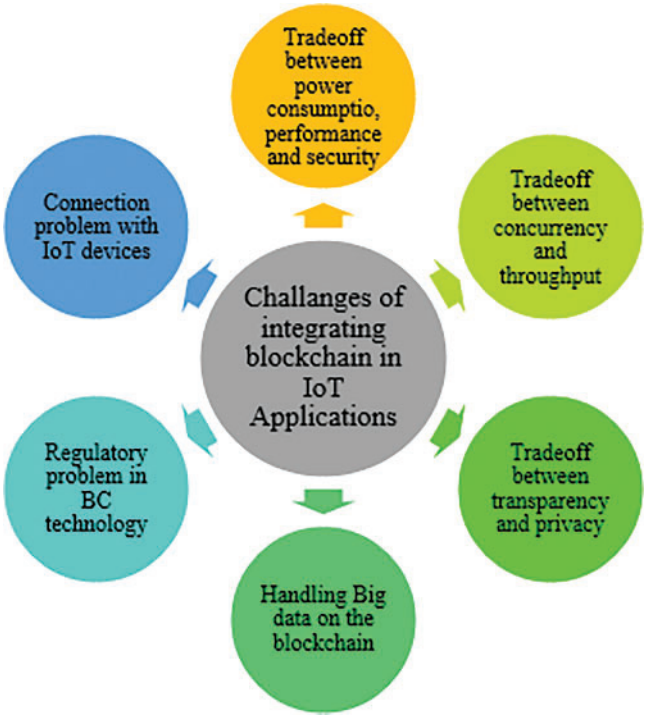

Figure 11: The challenges of integrating blockchain in IoT applications

Table 5: Solutions for IoT and blockchain integrating challenges

	Challenges	Issues	Solutions
1	Scalability	Limited scalability due to high data volume	Use lightweight consensus mechanisms like Proof of Authority (PoA) or Delegated Proof of Stake (DPoS) to enhance scalability in IoT environments [182].
2	Latency	Latency in data processing and transmission	• Utilizing Edge Computing and Fog Computing to process data closer to the source and minimize delays [183]. • Implement off-chain solutions or sidechains to reduce the delay in transaction processing, enabling real-time IoT interactions [184].
3	Energy consumption	• High Energy consumption and computational power in Consensus Mechanisms • Power limitations of IoT devices	Use energy-efficient consensus algorithms such as Proof of Stake (PoS) to minimize the energy requirements of IoT devices [185].

(Continued)

Table 5 (continued)

	Challenges	Issues	Solutions
4	Security	Security vulnerabilities (e.g., unauthorized access, hacking, and Sybil attacks)	Implementing robust authentication mechanisms, multi-signature schemes, and intrusion detection systems to prevent unauthorized access [186].
5	Data privacy	Privacy concerns (e.g., exposure of sensitive data and user identity leaks)	Utilizing encryption techniques such as zero-knowledge proofs (ZKPs) and homomorphic encryption to ensure privacy while maintaining transparency [187].
6	Interoperability	Lack of standardization across devices	Develop standardized communication protocols and use blockchain interoperability layers to enable IoT devices from different manufacturers to communicate seamlessly [21].
7	Cost	High implementation and operational costs	Use hybrid blockchain models that combine private and public blockchains to optimize costs while ensuring security and scalability [188].
8	Device management	Device management challenges (e.g., handling a large number of IoT devices, firmware updates, and identity management)	Implement decentralized identity management systems and automated smart contracts for secure and efficient IoT device management [189].

6 Future Research Direction

The potential of this integration has been investigated in many studies, which have also suggested future lines of inquiry in this area. Researchers from various parts of the globe are actively working on exploring and creating innovative methods to incorporate blockchain technology into the IoT ecosystem. The aim is to leverage the potential of blockchain to enhance the functionality, security, and efficiency of IoT devices and networks. Using the blockchain can solve many problems in the IoT network, so the blockchain provides a reliable encryption system. As a result, the performance of network security has improved. While the IoT network's integration with blockchain addresses certain issues, it also introduces new ones, including higher transaction latency and network communication overhead and more difficult management and monitoring of large networks.

While there are numerous advantages to integrating IoT and blockchain in terms of enhancing data security, integrity, and transparency, consideration must also be given to how it is implemented. Future research could concentrate on tackling particular issues like boosting throughput and scalability and investigating the possible uses of these integrated technologies across a range of industries [190]. Energy efficiency is one of the primary concerns in blockchain networks; since IoT networks have limited resources, research into hybrid consensus mechanisms and energy-efficient protocols to lower energy consumption can be considered future work [191].

To provide a roadmap for future work, hardware-based security solutions, improved consensus algorithms, and the use of trendy technologies like machine learning and artificial intelligence to combat sophisticated cyberattacks are all being considered. To fill these gaps, future studies will examine attacker behavior, lower modeling costs, and develop new approaches to scalability, computational overhead reduction, and BIoT component integration [46].

Future research can focus on implementing the blockchain-based system in real-world Internet of Things environments. This will entail tackling issues like scalability, maintenance expenses, and deployment. Additionally, it investigates how the system can be modified to fit various IoT infrastructures [158]. Future research should concentrate on improving blockchain technology for IoT environments, creating powerful consensus methods, and developing new interoperability standards [192].

According to our review, we can see that scalability issues with IoT and blockchain integration have been the subject of very little research; thus, it is still in its infancy. As blockchain technology opens up new IoT markets, it is also possible to introduce a variety of blockchain applications in the IoT [193]. Future research can be done to address the primary issues with integrating blockchain with the Internet of Things, which include blockchain scalability, energy consumption, integration complexity, regulatory compliance, security and privacy, cost, and centralization [194].

7 Conclusion

In this paper, we analyze in detail the impact of blockchain technology on the Internet of Things. We first examined the effect of blockchain on the IoT and then identified the challenges that stand in the way of the broad adoption of blockchain in the IoT. Additionally, we engaged in an in-depth review of various applications that combine blockchain and IoT to shed light on emerging trends in IoT applications and how these applications address the issues associated with blockchain implementation. This article presents the challenges blockchain and the Internet of Things should face to cooperate successfully. Blockchain can play an effective role in enhancing IoT applications.

We have conferred on IoT applications. IoT devices have constrained resources. While blockchain has much computing power, blockchain and Internet of Things integration present several difficulties. In addition, IoT systems based on blockchain are susceptible to several privacy risks, which must be addressed before they are used.

This survey examines the problems with IoT integration and offers pertinent solutions from the literature. Additionally, we have provided suggestions for future IoT integration research directions. Because the integration of blockchain and the Internet of Things has attracted much attention in science and business, other technologies are likely to influence their development and growth. Due to this integration, there is also the possibility that services and applications will emerge in the future. We also looked at blockchain's advantages for IoT problems.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm contribution to the paper as follows: Study conception and design, collection, analysis and interpretation of results, draft manuscript preparation: Mozhgan Gholami. Review, editing, and supervision paper: Ali Ghaffari, Nahideh Derakhshanfard, Nadir iBRAHIMOĞLU, and Ali Asghar Pourhaji Kazem. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest to report regarding the present study.

Abbreviation

IoT	Internet of Things
BCN	Blockchain Network
P2P	Peer to Peer
SDN	Software Defined Network
FC	Fog Computing
DDoS	Distributed Denial of Service
FT	Fault Tolerance
PoA	Proof of Authority
DLT	Distributed Ledger Technology
TX	Transaction
IPFS	Interplanetary File System
QoS	Quality of Services
BCoT	BC of Things
IoE	Internet of Everything
SC	Smart Contract
DL	Deep Learning
DTL	Decentralized Technology Landscape
BIoT	Blockchain IoT
Wi-Fi	Wireless Fidelity
WSN	Wireless Sensor Network
IDS	Intrusion Detection System
IP	Internet Protocol
BcoT	Blockchain of Things
IIoT	Industrial IoT
DC	Distributed Computing
PoW	Proof-of-Work
IOTA	Internet of Things Association
PoET	Proof of Elapsed Time
WSN	Wireless Sensor Network
PoS	Proof of Stake
DTL	Distributed Transaction Ledger
RFID	Radio-Frequency Identification
BASN	Body Area Sensor Networks
FL	Federated Learning
HIoT	Healthcare IoT
SMR	State Machine Replication

References

1. Mohanta BK, Jena D, Satapathy U, Patnaik S. Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet Things. 2020;11(8):100227. doi:10.1016/j.iot.2020.100227.
2. Hanafi AV, Ghaffari A, Rezaei H, Valipour A, Arasteh B. Intrusion detection in Internet of Things using improved binary golden jackal optimization algorithm and LSTM. Clust Comput. 2024;27(3):2673–90. doi:10.1007/s10586-023-04102-x.

3. Nematollahi M, Ghaffari A, Mirzaei A. Task and resource allocation in the Internet of Things based on an improved version of the moth-flame optimization algorithm. Clust Comput. 2024;27(2):1775–97. doi:10.1007/s10586-023-04041-7.
4. Nematollahi M, Ghaffari A, Mirzaei A. Task offloading in Internet of Things based on the improved multi-objective *Aquila* optimizer. Signal Image Video Process. 2024;18(1):545–52. doi:10.1007/s11760-023-02761-2.
5. Pavithra PS, Durgadevi P. Improving security: blockchain based IoT solutions for the healthcare. J Theor Appl Inform Technol. 2024;102(6):2716–25.
6. Atlam HF, Alenezi A, Alharthi A, Walters RJ, Wills GB. Integration of cloud computing with Internet of Things: challenges and open issues. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); 2017 Jun 21–23; Exeter, UK: IEEE; 2017. p. 670–5. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.105.
7. Kala MK, Priya M. A comprehensive survey on the IoT-based electronic healthcare records security, privacy issues, and countermeasures using blockchain technology. In: 2023 International Conference on Innovations in Engineering and Technology (ICIET); 2023 Jul 13–14; Muvattupuzha, India: IEEE; 2023. p. 1–8. doi:10.1109/ICIET57285.2023.10220624.
8. Gong Y, Yao H, Nallanathan A. Intelligent sensing, communication, computation, and caching for satellite-ground integrated networks. IEEE Netw. 2024;38(4):9–16. doi:10.1109/MNET.2024.3413543.
9. Samizadeh Nikoui T, Rahmani AM, Balador A, Haj Seyyed Javadi H. Internet of Things architecture challenges: a systematic review. Int J Communication. 2021;34(4):e4678. doi:10.1002/dac.4678.
10. Allam AH, Gomaa I, Zayed HH, Taha M. IoT-based eHealth using blockchain technology: a survey. Clust Comput. 2024;27(6):7083–110. doi:10.1007/s10586-024-04357-y.
11. Ghaffari A, Jelodari N, Pouralish S, Derakhshanfard N, Arasteh B. Securing internet of things using machine and deep learning methods: a survey. Clust Comput. 2024;27(7):9065–89. doi:10.1007/s10586-024-04509-0.
12. Nazir A, He J, Zhu N, Anwar MS, Pathan MS. Enhancing IoT security: a collaborative framework integrating federated learning, dense neural networks, and blockchain. Clust Comput. 2024;27(6):8367–92. doi:10.1007/s10586-024-04436-0.
13. Asgharzadeh H, Ghaffari A, Masdari M, Soleimanian Gharehchopogh F. Anomaly-based intrusion detection system in the Internet of Things using a convolutional neural network and multi-objective enhanced Capuchin Search Algorithm. J Parallel Distrib Comput. 2023;175(5):1–21. doi:10.1016/j.jpdc.2022.12.009.
14. Seyfollahi A, Taami T, Ghaffari A. Towards developing a machine learning-metaheuristic-enhanced energy-sensitive routing framework for the Internet of Things. Microprocess Microsyst. 2023;96(2):104747. doi:10.1016/j.micpro.2022.104747.
15. Asgharzadeh H, Ghaffari A, Masdari M, Gharehchopogh FS. An intrusion detection system on the Internet of Things using deep learning and multi-objective enhanced *Gorilla* troops optimizer. J Bionic Eng. 2024;21(5):2658–84. doi:10.1007/s42235-024-00575-7.
16. Zhang L, Yao Z, Zhang B, Li C. Scalable creditable-committee-based blockchain consensus protocol for multihop wireless networks. IEEE Internet Things J. 2024;11(18):29628–42. doi:10.1109/JIOT.2024.3393927.
17. Mousavi SK, Ghaffari A, Besharat S, Afshari H. Improving the security of Internet of Things using cryptographic algorithms: a case of smart irrigation systems. J Ambient Intell Humaniz Comput. 2021;12(2):2033–51. doi:10.1007/s12652-020-02303-5.
18. Mousavi SK, Ghaffari A, Besharat S, Afshari H. Security of Internet of Things using RC4 and ECC algorithms (case study: smart irrigation systems). Wirel Pers Commun. 2021;116(3):1713–42. doi:10.1007/s11277-020-07758-5.
19. Seyfollahi A, Ghaffari A. A review of intrusion detection systems in RPL routing protocol based on machine learning for Internet of Things applications. Wirel Commun Mob Comput. 2021;2021(1):8414503. doi:10.1155/2021/8414503.
20. Alkadi O, Moustafa N, Turnbull B, Choo KR. A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks. IEEE Internet Things J. 2021;8(12):9463–72. doi:10.1109/JIOT.2020.2996590.

21. Panarello A, Tapas N, Merlino G, Longo F, Puliafito A. Blockchain and IoT integration: a systematic survey. Sensors. 2018;18(8):2575. doi:10.3390/s18082575.
22. Jazebi SJ, Ghaffari A. *RISA*: routing scheme for Internet of Things using shuffled frog leaping optimization algorithm. J Ambient Intell Humaniz Comput. 2020;11(10):4273–83. doi:10.1007/s12652-020-01708-6.
23. Seyfollahi A, Ghaffari A. Reliable data dissemination for the Internet of Things using Harris Hawks optimization. Peer Peer Netw Appl. 2020;13(6):1886–902. doi:10.1007/s12083-020-00933-2.
24. Mousavi SK, Ghaffari A. Data cryptography in the Internet of Things using the artificial bee colony algorithm in a smart irrigation system. J Inf Secur Appl. 2021;61(1):102945. doi:10.1016/j.jisa.2021.102945.
25. Sudha MK, Manorama M, Aditi T. Smart agricultural decision support systems for predicting soil nutrition value using IoT and ridge regression. Agris Line Pap Econ Inform. 2022;14(1):95–106. doi:10.7160/aol.2022.140108.
26. Sun G, Xu Z, Yu H, Chang V. Dynamic network function provisioning to enable network in box for industrial applications. IEEE Trans Ind Inform. 2021;17(10):7155–64. doi:10.1109/TII.2020.3042872.
27. Adhikari N, Ramkumar M. IoT and blockchain integration: applications, opportunities, and challenges. Network. 2023;3(1):115–41. doi:10.3390/network3010006.
28. Yazdinejad A, Dehghantanha A, Parizi RM, Srivastava G, Karimipour H. Secure intelligent fuzzy blockchain framework: effective threat detection in IoT networks. Comput Ind. 2023;144(4):103801. doi:10.1016/j.compind.2022.103801.
29. Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview. arXiv:1906.11078. 2019.
30. Luo H, Zhang Q, Sun G, Yu H, Niyato D. Symbiotic blockchain consensus: cognitive backscatter communications-enabled wireless blockchain consensus. IEEE/ACM Trans Netw. 2024;32(6):5372–87. doi:10.1109/TNET.2024.3462539.
31. Lee B, Lee JH. Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. J Supercomput. 2017;73(3):1152–67. doi:10.1007/s11227-016-1870-0.
32. Khan A, Laghari A, Awan S. Machine learning in computer vision: a review. EAI Endorsed Transact Scal Inform Syst. 2021;8(32):e4. doi:10.4108/eai.21-4-2021.169418.
33. Franco J, Aris A, Canberk B, Uluagac AS. A survey of honeypots and honeynets for Internet of Things, industrial Internet of Things, and cyber-physical systems. IEEE Commun Surv Tutor. 2021;23(4):2351–83. doi:10.1109/COMST.2021.3106669.
34. Jiang B, Li J, Yue G, Song H. Differential privacy for industrial Internet of Things: opportunities, applications, and challenges. IEEE Internet Things J. 2021;8(13):10430–51. doi:10.1109/JIOT.2021.3057419.
35. Ayub Khan A, Ali Laghari A, Shaikh AA, Bourouis S, Mamlouk AM, Alshazly H. Educational blockchain: a secure degree attestation and verification traceability architecture for higher education commission. Appl Sci. 2021;11(22):10917. doi:10.3390/app112210917.
36. Kumar RL, Khan F, Kadry S, Rho S. A survey on blockchain for industrial Internet of Things. Alex Eng J. 2022;61(8):6001–22. doi:10.1016/j.aej.2021.11.023.
37. Sharma M, Pant S, Kumar Sharma D, Datta Gupta K, Vashishth V, Chhabra A. Enabling security for the Industrial Internet of Things using deep learning, blockchain, and coalitions. Trans Emerging Tel Tech. 2021;32(7):e4137. doi:10.1002/ett.4137.
38. Abed S, Jaffal R, Mohd BJ. A review on blockchain and IoT integration from energy, security and hardware perspectives. Wirel Pers Commun. 2023;129(3):2079–122. doi:10.1007/s11277-023-10226-5.
39. Kshetri N. Can blockchain strengthen the Internet of Things? IT Profess. 2017;19(4):68–72. doi:10.1109/MITP.2017.3051335.
40. Al Sadawi A, Hassan MS, Ndiaye M. A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. IEEE Access. 2021;9:54478–97. doi:10.1109/ACCESS.2021.3070555.
41. Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener Comput Syst. 2018;88(3):173–90. doi:10.1016/j.future.2018.05.046.
42. Dai HN, Zheng Z, Zhang Y. Blockchain for internet of things: a survey. IEEE Internet Things J. 2019;6(5):8076–94. doi:10.1109/JIOT.2019.2920987.

43. Wang X, Zha X, Ni W, Liu RP, Guo YJ, Niu X, et al. Survey on blockchain for Internet of Things. Comput Commun. 2019;136(7):10–29. doi:10.1016/j.comcom.2019.01.006.
44. Huan NTY, Ahmad Zukarnain Z. A survey on addressing IoT security issues by embedding blockchain technology solutions: review, attacks, current trends, and applications. IEEE Access. 2024;12(3):69765–82. doi:10.1109/ACCESS.2024.3378592.
45. Fazel E, Nezhad MZ, Rezazadeh J, Moradi M, Ayoade J. IoT convergence with machine learning & blockchain: a review. Internet Things. 2024;26(24):101187. doi:10.1016/j.iot.2024.101187.
46. Commey D, Mai B, Hounsinou SG, Crosby GV. Securing blockchain-based IoT systems: a review. IEEE Access. 2024;12(8):98856–81. doi:10.1109/ACCESS.2024.3428490.
47. Xu LD, Lu Y, Li L. Embedding blockchain technology into IoT for security: a survey. IEEE Internet Things J. 2021;8(13):10452–73. doi:10.1109/JIOT.2021.3060508.
48. Cirne A, Sousa PR, Resende JS, Antunes L. IoT security certifications: challenges and potential approaches. Comput Secur. 2022;116(15):102669. doi:10.1016/j.cose.2022.102669.
49. Makhdoom I, Abolhasan M, Abbas H, Ni W. Blockchain's adoption in IoT: the challenges, and a way forward. J Netw Comput Appl. 2019;125(9):251–79. doi:10.1016/j.jnca.2018.10.019.
50. Choudhary A. Internet of Things: a comprehensive overview, architectures, applications, simulation tools, challenges and future directions. Discov Internet Things. 2024;4(1):31. doi:10.1007/s43926-024-00084-3.
51. Díaz M, Martín C, Rubio B. State-of-the-art, challenges, and open issues in the integration of Internet of Things and cloud computing. J Netw Comput Appl. 2016;67(7):99–117. doi:10.1016/j.jnca.2016.01.010.
52. Xiao J, Ren Y, Du J, Zhao Y, Kumari S, Alenazi MJF, et al. CALRA: practical conditional anonymous and leakage-resilient authentication scheme for vehicular crowdsensing communication. IEEE Trans Intell Transp Syst. 2025;26(1):1273–85. doi:10.1109/TITS.2024.3488741.
53. Wang Y, Sun R, Cheng Q, Ochieng WY. Measurement quality control aided multisensor system for improved vehicle navigation in urban areas. IEEE Trans Ind Electron. 2023;71(6):6407–17. doi:10.1109/TIE.2023.3288188.
54. Tariq N, Qamar A, Asim M, Khan FA. Blockchain and smart healthcare security: a survey. Procedia Comput Sci. 2020;175(9):615–20. doi:10.1016/j.procs.2020.07.089.
55. Xiao X, He Q, Li Z, Antoce AO, Zhang X. Improving traceability and transparency of table grapes cold chain logistics by integrating WSN and correlation analysis. Food Contr. 2017;73(8):1556–63. doi:10.1016/j.foodcont.2016.11.019.
56. Xu G, Kong DL, Zhangs K, Xu S, Cao Y, Mao Y, et al. A model value transfer incentive mechanism for federated learning with smart contracts in AIoT. IEEE Internet Things J. 2024;12(3):2530–44. doi:10.1109/JIOT.2024.3468443.
57. Wang E, Yang Y, Wu J, Liu W, Wang X. An efficient prediction-based user recruitment for mobile crowdsensing. IEEE Trans Mob Comput. 2018;17(1):16–28. doi:10.1109/TMC.2017.2702613.
58. Gong J, Yu Q, Li T, Liu H, Zhang J, Fan H, et al. Demo: scalable digital twin system for mobile networks with generative AI. In: Proceedings of the 21st Annual International Conference on Mobile Systems, Applications and Services (MobiSys' 23); 2023; Helsinki, Finland. p. 610–1. doi:10.1145/3581791.3597297.
59. Liu L, Zhou B, Zou Z, Yeh SC, Zheng L. A smart unstaffed retail shop based on artificial intelligence and IoT. In: 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD); 2018 Sep 17–19; Barcelona, Spain: IEEE; 2018. p. 1–4. doi:10.1109/CAMAD.2018.8514988.
60. Radoglou Grammatikis PI, Sarigiannidis PG, Moscholios ID. Securing the Internet of Things: challenges, threats and solutions. Internet Things. 2019;5(7):41–70. doi:10.1016/j.iot.2018.11.003.
61. Li C, He A, Liu G, Wen Y, Chronopoulos AT, Giannakos A. RFL-*APIA*: a comprehensive framework for mitigating poisoning attacks and promoting model aggregation in IIoT federated learning. IEEE Trans Ind Inform. 2024;20(11):12935–44. doi:10.1109/TII.2024.3431020.
62. Zhang D, Le J, Mu N, Liao X. An anonymous off-blockchain micropayments scheme for cryptocurrencies in the real world. IEEE Trans Syst Man Cybern Syst. 2020;50(1):32–42. doi:10.1109/TSMC.2018.2884289.
63. Yang Y, Wu L, Yin G, Li L, Zhao H. A survey on security and privacy issues in Internet-of-things. IEEE Internet Things J. 2017;4(5):1250–8. doi:10.1109/JIOT.2017.2694844.

64. Adele G, Borah A, Paranjothi A, Khan MS, Poulkov VK. A comprehensive systematic review of blockchain-based intrusion detection systems. In: 2024 IEEE World AI IoT Congress (AIIoT); 2024 May 29–31; Seattle, WA, USA: IEEE; 2024. p. 605–11. doi:10.1109/AIIoT61789.2024.10578958.
65. Jiang H, Ji P, Zhang T, Cao H, Liu D. Two-factor authentication for keyless entry system *via* finger-induced vibrations. IEEE Trans Mob Comput. 2024;23(10):9708–20. doi:10.1109/TMC.2024.3368331.
66. Zandberg K, Schleiser K, Acosta F, Tschofenig H, Baccelli E. Secure firmware updates for constrained IoT devices using open standards: a reality check. IEEE Access. 2019;7:71907–20. doi:10.1109/ACCESS.2019.2919760.
67. Qiao Y, Lü J, Wang T, Liu K, Zhang B, Snoussi H. A multihead attention self-supervised representation model for industrial sensors anomaly detection. IEEE Trans Ind Inform. 2024;20(2):2190–9. doi:10.1109/TII.2023.3280337.
68. Chen Y, Bellavitis C. Blockchain disruption and decentralized finance: the rise of decentralized business models. J Bus Ventur Insights. 2020;13(2):e00151. doi:10.1016/j.jbvi.2019.e00151.
69. Bhushan B, Sahoo C, Sinha P, Khamparia A. Unification of blockchain and Internet of Things (BIoT): requirements, working model, challenges and future directions. Wirel Netw. 2021;27(1):55–90. doi:10.1007/s11276-020-02445-6.
70. Tseng L, Wong L, Otoum S, Aloqaily M, Ben Othman J. Blockchain for managing heterogeneous Internet of Things: a perspective architecture. IEEE Netw. 2020;34(1):16–23. doi:10.1109/MNET.001.1900103.
71. Bhushan B, Sinha P, Sagayam KM, Andrew J. Untangling blockchain technology: a survey on state of the art, security threats, privacy services, applications and future research directions. Comput Electr Eng. 2021;90(9):106897. doi:10.1016/j.compeleceng.2020.106897.
72. Ramkumar M, Adhikari N. Blockchain based redistricting with public participation. J Inf Secur. 2022;13(3):140–64. doi:10.4236/jis.2022.133009.
73. Schollmeier R. A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. In: Proceedings First International Conference on Peer-to-Peer Computing; 2001 Aug 27–29; Linköping, Sweden: IEEE; 2002. p. 101–2. doi:10.1109/P2P.2001.990434.
74. Yang J, Yang K, Xiao Z, Jiang H, Xu S, Dustdar S. Improving commute experience for private car users *via* blockchain-enabled multitask learning. IEEE Internet Things J. 2023;10(24):21656–69. doi:10.1109/JIOT.2023.3317639.
75. Liu J, Chen C, Li Y, Sun L, Song Y, Zhou J, et al. Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning. Knowl Inf Syst. 2024;66(8):4377–403. doi:10.1007/s10115-024-02117-3.
76. Ali MS, Vecchio M, Pincheira M, Dolui K, Antonelli F, Rehmani MH. Applications of blockchains in the Internet of Things: a comprehensive survey. IEEE Commun Surv Tutor. 2018;21(2):1676–717. doi:10.1109/COMST.2018.2886932.
77. Beck R, Avital M, Rossi M, Thatcher JB. Blockchain technology in business and information systems research. Bus Inf Syst Eng. 2017;59(6):381–4. doi:10.1007/s12599-017-0505-1.
78. Hofmann E, Strewe UM, Bosia N. Supply chain finance and blockchain technology: the case of reverse securitisation. 1st ed. Berlin/Heidelberg, Germany: Springer; 2017.
79. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the Internet of Things. IEEE Access. 2016;4:2292–303. doi:10.1109/ACCESS.2016.2566339.
80. Shen J, Sheng H, Wang S, Cong R, Yang D, Zhang Y. Blockchain-based distributed multiagent reinforcement learning for collaborative multiobject tracking framework. IEEE Trans Comput. 2024;73(3):778–88. doi:10.1109/TC.2023.3343102.
81. Gong Y, Yao H, Xiong Z, Philip Chen CL, Niyato D. Blockchain-aided digital twin offloading mechanism in space-air-ground networks. IEEE Trans Mob Comput. 2025;24(1):183–97. doi:10.1109/TMC.2024.3455417.
82. Liu Y, Zhao Y. A blockchain-enabled framework for vehicular data sensing: enhancing information freshness. IEEE Trans Veh Technol. 2024;73(11):17416–29. doi:10.1109/TVT.2024.3417689.
83. Jebri S, Ben Amor A, Zidi S. A seamless authentication for intra and inter metaverse platforms using blockchain. Comput Netw. 2024;247(1):110460. doi:10.1016/j.comnet.2024.110460.
84. Wen F. The new trend of the integration of artificial intelligence and blockchain in network security. Acad J Comput Inf Sci. 2024;7(3):38–42. doi:10.25236/ajcis.2024.070305.

85. Xiong H, Gong L, Li R, Kumari S, Chen CM, Amoon M. Blockchain-enabled distributed identity-based ring signature with identity abort for consumer electronics. IEEE Trans Consum Electron. 2024;70(3):5340–52. doi:10.1109/TCE.2024.3426101.
86. Singh S, Gupta A, Chaudhary A. Enhancing Blockchain Security through quantum key distribution and evaluating QKD network in QKDNetSim environment. In: 2024 3rd International Conference on Power Electronics and IoT Applications in Renewable Energy and Its Control (PARC); 2024 Feb 23–24; Mathura, India: IEEE; 2024. p. 86–93. doi:10.1109/PARC59193.2024.10486256.
87. Pongnumkul S, Siripanpornchana C, Thajchayapong S. Performance analysis of private blockchain platforms in varying workloads. In: 2017 26th International Conference on Computer Communication and Networks (ICCCN); 2017 Jul 31–Aug 3; Vancouver, BC, Canada: IEEE; 2017. p. 1–6. doi:10.1109/ICCCN.2017.8038517.
88. Alfandi O, Khanji S, Ahmad L, Khattak A. A survey on boosting IoT security and privacy through blockchain. Clust Comput. 2021;24(1):37–55. doi:10.1007/s10586-020-03137-8.
89. Saad M, Spaulding J, Njilla L, Kamhoua C, Shetty S, Nyang D, et al. Exploring the attack surface of blockchain: a systematic overview. arXiv:1904.03487. 2019.
90. Lao L, Li Z, Hou S, Xiao B, Guo S, Yang Y. A survey of IoT applications in blockchain systems. ACM Comput Surv. 2021;53(1):1–32. doi:10.1145/3372136.
91. Liang X, Shetty S, Tosh D, Kamhoua C, Kwiat K, Njilla L. ProvChain: a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In: 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID); 2017 May 14–17; Madrid, Spain: IEEE; 2017. p. 468–77. doi:10.1109/CCGRID.2017.8.
92. Behnke K, Janssen MFWHA. Boundary conditions for traceability in food supply chains using blockchain technology. Int J Inf Manag. 2020;52(9):101969. doi:10.1016/j.ijinfomgt.2019.05.025.
93. Helliar CV, Crawford L, Rocca L, Teodori C, Veneziani M. Permissionless and permissioned blockchain diffusion. Int J Inf Manag. 2020;54(3):102136. doi:10.1016/j.ijinfomgt.2020.102136.
94. Liu M, Wu K, Xu JJ. How will blockchain technology impact auditing and accounting: permissionless versus permissioned blockchain. Curr Issues Auditing. 2019;13(2):A19–29. doi:10.2308/ciia-52540.
95. Staples M, Chen S, Falamaki S, Ponomarev A, Rimba P, Tran A, et al. Risks and opportunities for systems using blockchain and smart contracts. Data61. Sydney, NSW, Austrilia: CSIRO. Report number: EP175103. 2017.
96. Polge J, Robert J, Le Traon Y. Permissioned blockchain frameworks in the industry: a comparison. ICT Express. 2021;7(2):229–33. doi:10.1016/j.icte.2020.09.002.
97. Amiri MJ, Agrawal D, El Abbadi A. Permissioned blockchains: properties, techniques and applications. In: Proceedings of the 2021 International Conference on Management of Data; 2021; Virtual Event, China: ACM. p. 2813–20. doi:10.1145/3448016.
98. Ahsan MS, Pathan A-SK. The state-of-the-art access control models in IoT: a survey on the requirements, scale, and future challenges. 2024. doi:10.2139/ssrn.4907677.
99. Maroufi M, Abdolee R, Tazekand BM. On the convergence of blockchain and Internet of Things (IoT) technologies. arXiv:1904.01936. 2019.
100. Torky M, Hassanein AE. Integrating blockchain and the Internet of Things in precision agriculture: analysis, opportunities, and challenges. Comput Electron Agric. 2020;178(2):105476. doi:10.1016/j.compag.2020.105476.
101. Suárez-Armas J, Caballero-Gil C, Rivero-García A, Caballero-Gil P. Authentication and encryption for a robotic ad hoc network using identity-based cryptography. In: 2018 4th International Conference on Big Data Innovations and Applications (Innovate-Data); 2018 Aug 6–8; Barcelona, Spain: IEEE; 2018. p. 71–6. doi:10.1109/Innovate-Data.2018.00018.
102. Theodorakopoulos L, Theodoropoulou A, Halkiopoulos C. Enhancing decentralized decision-making with big data and blockchain technology: a comprehensive review. Appl Sci. 2024;14(16):7007. doi:10.3390/app14167007.
103. Potter K, Stilinski D, Adablanu S. Blockchain-based Security Solutions for the Internet of Things (IoT). EasyChair. 2024. Report No.: 2516–2314.
104. Guo H, Yu X. A survey on blockchain technology and its security. Blockchain Res Appl. 2022;3(2):100067. doi:10.1016/j.bcra.2022.100067.

105. Abd Ali SM, Yusoff MN, Hasan HF. Redactable blockchain: comprehensive review, mechanisms, challenges, open issues and future research directions. Future Internet. 2023;15(1):35. doi:10.3390/fi15010035.
106. Vukolić M. The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In: International Workshop on Open Problems in Network Security (iNetSec); 2015 Oct; Zurich, Switzerland. p. 112–25.
107. Hussein NH, Yaw CT, Koh SP, Tiong SK, Chong KH. A comprehensive survey on vehicular networking: communications, applications, challenges, and upcoming research directions. IEEE Access. 2022;10(6):86127–80. doi:10.1109/ACCESS.2022.3198656.
108. Henry R, Herzberg A, Kate A. Blockchain access privacy: challenges and directions. IEEE Secur Priv. 2018;16(4):38–45. doi:10.1109/MSP.2018.3111245.
109. Antonopoulos AM, Wood G. Mastering ethereum: building smart contracts and dapps. 1st ed. Sebastopol, CA, USA: O'reilly Media; 2018.
110. Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang FY. Blockchain-enabled smart contracts: architecture, applications, and future trends. IEEE Trans Syst Man Cybern Syst. 2019;49(11):2266–77. doi:10.1109/TSMC.2019.2895123.
111. Dhami A, Pareek PS, Maurya S, Matta P, Rawat V, Manu M. Application and issues of blockchain technology. In: 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA); 2023 Aug 3–5; Coimbatore, India: IEEE; 2023. p. 1283–8. doi:10.1109/ICIRCA57980.2023.10220723.
112. Abad-Segura E, Infante-Moro A, González-Zamar MD, López-Meneses E. Influential factors for a secure perception of accounting management with blockchain technology. J Open Innov Technol Mark Complex. 2024;10(2):100264. doi:10.1016/j.joitmc.2024.100264.
113. Thakur SN, Maurya S, Rawat B. A comprehensive study on blockchain: transforming the world. In: 2023 2nd International Conference for Innovation in Technology (INOCON); 2023 Mar 3–5; Bangalore, India: IEEE; 2023. p. 1–6. doi:10.1109/INOCON57975.2023.10101303.
114. Poon J, Buterin V. Plasma: scalable autonomous smart contracts. In: White paper; 2017 Aug. p. 1–47.
115. Sharma L, Olson J, Guha A, McDougal L. How blockchain will transform the healthcare ecosystem. Bus Horiz. 2021;64(5):673–82. doi:10.1016/j.bushor.2021.02.019.
116. He Y, Zhou Z, Pan Y, Chong F, Wu B, Xiao K, et al. Review of data security within energy blockchain: a comprehensive analysis of storage, management, and utilization. High Confid Comput. 2024;4(3):100233. doi:10.1016/j.hcc.2024.100233.
117. Chang Z, Guo W, Guo X, Chen T, Min G, Abualnaja KM, et al. Blockchain-empowered drone networks: architecture, features, and future. IEEE Netw. 2021;35(1):86–93. doi:10.1109/MNET.011.2000202.
118. Hasan MK, Zhou W, Safie N, Ahmed FRA, Ghazal TM. A survey on key agreement and authentication protocol for Internet of Things application. IEEE Access. 2024;12(7):61642–66. doi:10.1109/ACCESS.2024.3393567.
119. Dedeoglu V, Jurdak R, Putra GD, Dorri A, Kanhere SS. A trust architecture for blockchain in IoT. In: Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services; 2019; Houston, TX, USA: ACM. p. 190–9. doi:10.1145/3360774.3360822.
120. Lin C, He D, Huang X, Khan MK, Choo KR. DCAP: a secure and efficient decentralized conditional anonymous payment system based on blockchain. IEEE Trans Inf Forensics Secur. 2020;15:2440–52. doi:10.1109/TIFS.2020.2969565.
121. Wüst K, Gervais A. Do you need a blockchain?. In: 2018 Crypto Valley Conference on Blockchain Technology (CVCBT); 2018 Jun 20–22; Zug, Switzerland: IEEE; 2018. p. 45–54. doi:10.1109/CVCBT.2018.00011.
122. Ahmed MH. Integration of blockchain with the Internet of things: a systematic review. ScienceOpen Preprints. 2022 Nov 6.
123. Dorri A, Kanhere SS, Jurdak R, Gauravaram P. LSB: a lightweight scalable blockchain for IoT security and anonymity. J Parallel Distrib Comput. 2019;134(3):180–97. doi:10.1016/j.jpdc.2019.08.005.
124. Xu LD, Viriyasitavat W. Application of blockchain in collaborative Internet-of-things services. IEEE Trans Comput Soc Syst. 2019;6(6):1295–305. doi:10.1109/TCSS.2019.2913165.
125. Anwar M, Tariq N, Ashraf M, Moqurrab SA, Alabdullah B, Alsagri HS, et al. BBAD: blockchain-backed assault detection for cyber physical systems. IEEE Access. 2024;12(2):101878–94. doi:10.1109/ACCESS.2024.3404656.

126. Rai HM, Shukla KK, Tightiz L, Padmanaban S. Enhancing data security and privacy in energy applications: integrating IoT and blockchain technologies. Heliyon. 2024;10(19):e38917. doi:10.1016/j.heliyon.2024.e38917.
127. Bahga A. Blockchain platform for industrial internet of things. Wuhan, China: Scientific Research Publishing; 2016. Report No.: 1945–3124.
128. Huh S, Cho S, Kim S. Managing IoT devices using blockchain platform. In: 2017 19th International Conference on Advanced Communication Technology (ICACT); 2017 Feb 19–22; Pyeongchang, Republic of Korea: IEEE; 2017. p. 464–7.
129. Sharma PK, Singh S, Jeong YS, Park JH. DistBlockNet: a distributed blockchains-based secure SDN architecture for IoT networks. IEEE Commun Mag. 2017;55(9):78–85. doi:10.1109/MCOM.2017.1700041.
130. Lu Y, Xu LD. Internet of Things (IoT) cybersecurity research: a review of current research topics. IEEE Internet Things J. 2019;6(2):2103–15. doi:10.1109/JIOT.2018.2869847.
131. Gan S. An IoT simulator in NS3 and a key-based authentication architecture for IoT devices using blockchain [master's thesis]. Kanpur, India: Indian Institute of Technology; 2017.
132. Khan MA, Salah K. IoT security: review, blockchain solutions, and open challenges. Future Gener Comput Syst. 2018;82(15):395–411. doi:10.1016/j.future.2017.11.022.
133. Aazam M, Huh EN. Fog computing and smart gateway based communication for cloud of things. In: 2014 International Conference on Future Internet of Things and Cloud; 2014 Aug 27–29; Barcelona, Spain: IEEE; 2014. p. 464–70. doi:10.1109/FiCloud.2014.83.
134. Zhang Y, Li B, Liu B, Wu J, Wang Y, Yang X. An attribute-based collaborative access control scheme using blockchain for IoT devices. Electronics. 2020;9(2):285. doi:10.3390/electronics9020285.
135. Wu X, Kong F, Shi J, Bao L, Gao F, Li J. A blockchain Internet of Things data integrity detection model. In: Proceedings of the 1st International Conference on Advanced Information Science and System; 2019; Singapore Singapore: ACM. p. 1–7. doi:10.1145/3373477.3373498.
136. Baars D. Towards self-sovereign identity using blockchain technology [master's thesis]. Enschede, The Netherland: University of Twente; 2016.
137. Yang T, Guo Q, Tai X, Sun H, Zhang B, Zhao W, et al. Applying blockchain technology to decentralized operation in future energy Internet. In: 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2); 2017 Nov 26–28; Beijing, China: IEEE; 2017. p. 1–5. doi:10.1109/EI2.2017.8244418.
138. Ourad AZ, Belgacem B, Salah K. Using blockchain for IOT access control and authentication management. In: Internet of Things–ICIOT 2018. Cham: Springer International Publishing; 2018. p. 150–64. doi:10.1007/978-3-319-94370-1_11
139. Biswas K, Muthukkumarasamy V. Securing smart cities using blockchain technology. In: 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS); 2016 Dec 12–14; Sydney, NSW, Australia: IEEE; 2016. p. 1392–3. doi:10.1109/HPCC-SmartCity-DSS.2016.0198.
140. Zyskind G, Nathan O, Pentland A. Decentralizing privacy: using blockchain to protect personal data. In: 2015 IEEE Security and Privacy Workshops; 2015 May 21–22; San Jose, CA, USA: IEEE; 2015. p. 180–4. doi:10.1109/SPW.2015.27.
141. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommun Policy. 2017;41(10):1027–38. doi:10.1016/j.telpol.2017.09.003.
142. Dittmann G, Jelitto J. A blockchain proxy for lightweight IoT devices. In: 2019 Crypto Valley Conference on Blockchain Technology (CVCBT); 2019 Jun 24–26; Rotkreuz, Switzerland: IEEE; 2019. p. 82–5. doi:10.1109/cvcbt.2019.00015.
143. Son M, Kim H. Blockchain-based secure firmware management system in IoT environment. In: 2019 21st International Conference on Advanced Communication Technology (ICACT); 2019 Feb 17–20; Pyeongchang, Republic of Korea: IEEE; 2019. p. 142–6.
144. Huang C, Hu Y. BEAF: a blockchain and edge assistant framework with data sharing for IoT networks. In: 2020 IEEE/ACM Symposium on Edge Computing (SEC); 2020 Nov 12–14; San Jose, CA, USA: IEEE; 2020. p. 370–5. doi:10.1109/sec50012.2020.00054.

145. Kumar A, Chatterjee K. Securing Internet of medical devices using energy efficient blockchain for Healthcare 4.0. Clust Comput. 2024;27(6):8333–48. doi:10.1007/s10586-024-04437-z.
146. Hanafi AV, İbrahimoğlu N, Ghaffari A, Arasteh B. Hybrid of COOT optimization algorithm with genetic algorithm for sensor nodes clustering using software defined network. Wirel Pers Commun. 2024;138(3):1615–47. doi:10.1007/s11277-024-11563-9.
147. Sun S, Du R, Chen S, Li W. Blockchain-based IoT access control system: towards security, lightweight, and cross-domain. IEEE Access. 2021;9:36868–78. doi:10.1109/ACCESS.2021.3059863.
148. Gong Q, Zhang J, Wei Z, Wang X, Zhang X, Yan X, et al. SDACS: blockchain-based secure and dynamic access control scheme for Internet of Things. Sensors. 2024;24(7):2267. doi:10.3390/s24072267.
149. Sekhar GC, Aruna R. A novel blockchain-assisted deep learning model for secure edge intelligence in IoT networks. J Inst Eng Ind Ser C. 2024. doi:10.1007/s40032-024-01048-w.
150. Dange S, Nitnaware P. Secure share: optimal blockchain integration in IoT systems. J Comput Inf Syst. 2024;64(2):265–77. doi:10.1080/08874417.2023.2193943.
151. Li T, Liu A, Zhang S, Wang T, Song H. TCDT: a trust-enabled crowdsourced data trading system in intelligent blockchain over Internet of Things. Expert Syst Appl. 2025;265(3):125968. doi:10.1016/j.eswa.2024.125968.
152. Kashif M, Kalkan K. Differential privacy preserving based framework using blockchain for Internet-of-things. Peer Peer Netw Appl. 2024;18(1):33. doi:10.1007/s12083-024-01858-w.
153. Sasikumar A, Ravi L, Devarajan M, Selvalakshmi A, Turki Almaktoom A, Almazyad AS, et al. Corrections to blockchain-assisted hierarchical attribute-based encryption scheme for secure information sharing in industrial Internet of Things. IEEE Access. 2024;12:163197. doi:10.1109/ACCESS.2024.3486869.
154. Suneetha G, Haripriya D. An enhanced deep learning integrated blockchain framework for securing industrial IoT. Peer Peer Netw Appl. 2024;18(1):28. doi:10.1007/s12083-024-01857-x.
155. Ahamad D, Hameed SA. Two level blockchain-based privacy preservation framework in IoT with heuristic *fusi* on mechanism-aided deep learning architecture. Internet Things. 2023;24(10):100917. doi:10.1016/j.iot.2023.100917.
156. Zhang Y, Zhang P, Guizani M, Zhang J, Wang J, Zhu H, et al. Blockchain-based secure communication of Internet of Things in space-air-ground integrated network. Future Gener Comput Syst. 2024;158:391–9. doi:10.1016/j.future.2024.04.024.
157. Zhao W, Yang X, Qi S, Wei J, Dong X, Yang X, et al. Secure blockchain-based reputation system for IIoT-enabled retail industry with resistance to sybil attack. Future Gener Comput Syst. 2025;166(1–2):107705. doi:10.1016/j.future.2024.107705.
158. Meng Y, Wang B, Xing Q, Wang X, Liu J, Xu X. BBAD: blockchain-based data assured deletion and access control system for IoT. Peer Peer Netw Appl. 2024;18(2):101. doi:10.1007/s12083-024-01881-x.
159. Hussein DH, Houlahan E, Janelle-Goode A, Lumsden T, Ibnkahla M. A blockchain-based dual identity management and authentication framework for IoT networks. In: 2024 IEEE 10th World Forum on Internet of Things (WF-IoT); 2024 Nov 10–13; Ottawa, ON, Canada: IEEE; 2024. p. 544–9. doi:10.1109/WF-IoT62078.2024.10811126.
160. Özyilmaz KR, Yurdakul A. Integrating low–power IoT devices to a blockchain-based infrastructure: work-in-progress. In: Proceedings of the Thirteenth ACM International Conference on Embedded Software 2017 Companion; 2017 Oct 15. p. 1–2.
161. Panasenko S. An extension to the lightweight blockchain scheme for some cases of Internet of Things systems: a protocol for secure transferring IoT sensors between edge nodes. In: 2024 Conference on Information Communications Technology and Society (ICTAS); 2024 Mar 7–8; Durban, South Africa: IEEE; 2024. p. 128–32. doi:10.1109/ICTAS59620.2024.10507126.
162. Truby J. Decarbonizing Bitcoin: law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. Energy Res Soc Sci. 2018;44(3):399–410. doi:10.1016/j.erss.2018.06.009.
163. Zhou Z, Xie M, Zhu T, Xu W, Yi P, Huang Z, et al. EEP2P: an energy-efficient and economy-efficient P2P network protocol. In: International Green Computing Conference; 2014 Nov 3–5; Dallas, TX, USA: IEEE; 2014. p. 1–6. doi:10.1109/IGCC.2014.7039171.
164. King S, Nadal S. PPCoin: peer-to-peer crypto-currency with proof-of-stake.In: Self-published paper; 2019 Aug 19.

165. Dziembowski S, Faust S, Kolmogorov V, Pietrzak K. Proofs of space. In: Annual Cryptology Conference; Berlin/Heidelberg: Springer Berlin Heidelberg. 2015. p. 585–605.
166. França B. Homomorphic mini-blockchain scheme. HMBC pdf; 2015 Apr 24 [cited 2025 Feb 10]. Available from: https://cryptonite.info/files/HMBC.pdf.
167. Asolo B. Litecoin scrypt algorithm explained. 2018 [cited 2025 Feb 10]. Available from: https://www.mycryptopedia.com/litecoin-scrypt-algorithm-explained/.
168. Roman R, Lopez J, Mambo M. Mobile edge computing, fog et al. a survey and analysis of security threats and challenges. Future Gener Comput Syst. 2018;78(4):680–98. doi:10.1016/j.future.2016.11.009.
169. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed Internet of Things. Comput Netw. 2013;57(10):2266–79. doi:10.1016/j.comnet.2012.12.018.
170. Banerjee M, Lee J, Choo KR. A blockchain future for Internet of Things security: a position paper. Digit Commun Netw. 2018;4(3):149–60. doi:10.1016/j.dcan.2017.10.006.
171. Shen M, Deng Y, Zhu L, Du X, Guizani N. Privacy-preserving image retrieval for medical IoT systems: a blockchain-based approach. IEEE Netw. 2019;33(5):27–33. doi:10.1109/MNET.001.1800503.
172. Baliga A. Understanding blockchain consensus models. Persistent. 2017;4(1):14.
173. Uddin MA, Stranieri A, Gondal I, Balasubramanian V. An efficient selective miner consensus protocol in blockchain oriented IoT smart monitoring. In: 2019 IEEE International Conference on Industrial Technology (ICIT); 2019 Feb 13–15; Melbourne, Australia: IEEE; 2019. p. 1135–42. doi:10.1109/icit.2019.8754936.
174. Lashkari B, Musilek P. A comprehensive review of blockchain consensus mechanisms. IEEE Access. 2021;9:43620–52. doi:10.1109/ACCESS.2021.3065880.
175. Fahim S, Katibur Rahman SM, Mahmood S. Blockchain: a comparative study of consensus algorithms PoW, PoS, PoA. PoV Int J Math Sci Comput. 2023;9(3):46–57. doi:10.5815/ijmsc.2023.03.04.
176. Huang J, Kong L, Chen G, Wu MY, Liu X, Zeng P. Towards secure industrial IoT: blockchain system with credit-based consensus mechanism. IEEE Trans Ind Inform. 2019;15(6):3680–9. doi:10.1109/TII.2019.2903342.
177. Zhou Q, Huang H, Zheng Z, Bian J. Solutions to scalability of blockchain: a survey. IEEE Access. 2020;8:16440–55.
178. Sharma PK, Kumar N, Park JH. Blockchain technology toward green IoT: opportunities and challenges. IEEE Netw. 2020;34(4):263–9. doi:10.1109/MNET.001.1900526.
179. Agrawal R, Singhal S, Sharma A. Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm. Clust Comput. 2024;27(6):8015–30. doi:10.1007/s10586-024-04411-9.
180. Uddin MA, Stranieri A, Gondal I, Balasubramanian V. A survey on the adoption of blockchain in IoT: challenges and solutions. Blockchain Res Appl. 2021;2(2):100006. doi:10.1016/j.bcra.2021.100006.
181. Ellul J, Galea J, Ganado M, McCarthy S, Pace GJ. Regulating blockchain, DLT and smart contracts: a technology regulator's perspective. ERA Forum. 2020;21(2):209–20. doi:10.1007/s12027-020-00617-7.
182. Haque EU, Shah A, Iqbal J, Ullah SS, Alroobaea R, Hussain S. A scalable blockchain based framework for efficient IoT data management using lightweight consensus. Sci Rep. 2024;14(1):7841. doi:10.1038/s41598-024-58578-7.
183. Yousefpour A, Fung C, Nguyen T, Kadiyala K, Jalali F, Niakanlahiji A, et al. All one needs to know about fog computing and related edge computing paradigms: a complete survey. J Syst Archit. 2019;98(2011):289–330. doi:10.1016/j.sysarc.2019.02.009.
184. Gai F, Niu J, Ali Tabatabaee S, Feng C, Jalalzai M. Cumulus: a secure BFT-based sidechain for off-chain scaling. In: 2021 IEEE/ACM 29th International Symposium on Quality of Service (IWQOS); 2001 Jun 25–28; Tokyo, Japan: IEEE; 2021. p. 1–6. doi:10.1109/iwqos52092.2021.9521363.
185. Wadhwa S, Rani S, Kavita, Verma S, Shafi J, Wozniak M. Energy efficient consensus approach of blockchain for IoT networks with edge computing. Sensors. 2022;22(10):3733. doi:10.3390/s22103733.
186. Alajlan R, Alhumam N, Frikha M. Cybersecurity for blockchain-based IoT systems: a review. Appl Sci. 2023;13(13):7432. doi:10.3390/app13137432.
187. Zhou L, Diro A, Saini A, Kaisar S, Hiep PC. Leveraging zero knowledge proofs for blockchain-based identity sharing: a survey of advancements, challenges and opportunities. J Inf Secur Appl. 2024;80(6):103678. doi:10.1016/j.jisa.2023.103678.

188. Mercan S, Cebe M, Tekiner E, Akkaya K, Chang M, Uluagac S. A cost-efficient IoT forensics framework with blockchain. In: 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC); 2020 May 2–6; Toronto, ON, Canada: IEEE; 2020. p. 1–5. doi:10.1109/icbc48266.2020.9169397.
189. Ramírez-Gordillo T, Maciá-Lillo A, Pujol FA, García-D'Urso N, Azorín-López J, Mora H. Decentralized identity management for Internet of Things (IoT) devices using IOTA blockchain technology. Future Internet. 2025;17(1):49. doi:10.3390/fi17010049.
190. Admira TMA, Rahman P. Utilization of blockchain technology to improve security and transparency of information systems. Inf Technol Stud J. 2024;1(1):22–40. doi:10.62207/qtds0397.
191. Mondal S, Goswami SS. The evolution of blockchain technology: applications, challenges, and future directions. Decis Mak Adv. 2024;2(1):274–81. doi:10.31181/dma21202443.
192. Obaidat MA, Rawashdeh M, Alja'afreh M, Abouali M, Thakur K, Karime A. Exploring IoT and blockchain: a comprehensive survey on security, integration strategies, applications and future research directions. Big Data Cogn Comput. 2024;8(12):174. doi:10.3390/bdcc8120174.
193. Shammar EA, Zahary AT, Al-Shargabi AA. A survey of IoT and blockchain integration: security perspective. IEEE Access. 2021;9:156114–50. doi:10.1109/ACCESS.2021.3129697.
194. Khan I, Majib Y, Ullah R, Rana O. Blockchain applications for Internet of Things—a survey. Internet Things. 2024;27(5):101254. doi:10.1016/j.iot.2024.101254.