El Cezeri
Journal of Science and Engineering
ISSN: 2148-3736

Review Article

# Blockchain-based Internet of Things Security: A Survey

**Reem Alshamy[1a], Muhammet Ali Akcayol[2b]**
[1]Department of Computer Science, Institute of Informatics, Gazi University, Ankara, Türkiye
[2]Department of Computer Engineering, Faculty of Engineering, Gazi University, Ankara, Türkiye

rali.alshamy@gmail.com

DOI: 10.31202/ecjse.1804704
Received: 16.10.2025 Accepted: 19.01.2026
**How to cite this article:**
Alshamy R., Akcayol M. A., "Blockchain-based IoT Security: A Survey", El-Cezeri Journal of Science and Engineering, Vol: 13, Iss: 2, (2026), pp.(161-194).
ORCID: [a]0000-0003-0490-5387, [b]0000-0002-6615-1237.

**Abstract** The Internet of Things (IoT) has become a major issue that has gained significant attention in the research community. Advances in IoT technologies have resulted in the emergence of various security issues and raised concerns about potential privacy breaches of IoT data. Utilizing Blockchain Technology (BCT) is seen as a promising solution for addressing security issues in the IoT. This paper offers a clear overview of IoT security threats, including the related security characteristics and the challenges that come with integrating BCT with IoT. A brief discussion of various consensus protocols and existing security techniques is presented. A comparative study of several Distributed Ledger Technology (DLT) platforms based on both qualitative and quantitative evaluation criteria is also presented. This paper explores the role of BCT in improving security in Intrusion Detection Systems (IDS) and other applications in the IoT environment. Additionally, the paper identifies open issues and highlights potential research opportunities that can benefit future studies.

**Keywords:** Blockchain Technology, Distributed Ledger Technology, Internet of Things, Intrusion, Detection System.

## 1. INTRODUCTION

In recent years, the role of IoT in enabling innovative applications has increased. IoT transforms traditional systems into intelligent solutions through the integration of modern and sophisticated technologies, thereby improving efficiency and service quality. As IoT systems evolve to be more versatile, apprehensions over the privacy and security of IoT data are increasing. The smart devices employed in IoT design are inherently vulnerable and resource-constrained to numerous security threats. IoT devices interact via a centralized server, which heightens the risk of a single point of failure [1]. Every layer inside the IoT architecture encounters unique security challenges, complicating the development of a security model that accommodates the various components of the IoT framework. Moreover, security attacks targeting IoT architecture are growing in sophistication. Notable attacks include physical attacks, malicious node injection, phishing, impersonation, jamming, and data leakage [2]. Effectively countering security attacks in the IoT requires robust technological solutions. Security systems must meet essential criteria, including integrity, confidentiality, and availability. However, the high energy consumption and limited storage capacity of IoT devices make conventional cryptographic techniques insufficient for providing adequate security [3].

In light of these challenges, it is imperative to restructure and rethink IoT systems fundamentally. Currently, the most promising option for enabling a distributed and secure IoT environment is BCT [4]. Haber et al. first described BCT as "a cryptographically secured chain of blocks" in 1991 [5]. However, it obtained popularity once S. Nakamoto used it as a public ledger in the cryptocurrency Bitcoin (2008) [6]. Since then, it has drawn significant attention from a variety of fields, including insurance, transportation, banking, and agriculture. It helps make a number of processes quicker, leaner, and more transparent due to its effective transaction digitalization capabilities [7, 8]. BCT is a distributed ledger composed of cryptographically linked, timestamped blocks, allowing peers to share data transparently and securely. Accordingly, by utilizing a distributed and secure environment, BCT could overcome the security concerns related to traditional IoT systems. Many academic researchers are working to do away with the requirement for a central trusted authority and use BCT to enable IoT because of its decentralized, immutable, auditable, and fault-tolerant characteristics.

Recent research has explored the benefits of integrating BCT with the IoT in various scenarios. While some surveys have reviewed these solutions, they differ in the depth of their coverage of the topic. A thorough review is still needed to address the security concerns of BC-based IoT systems. This paper aims to address that need by examining the latest BCT that can enhance the security, performance, and efficiency of IoT, with a focus on recent research into security challenges in this area. Further, it identifies open research directions to guide future research. Table 1 summarizes our review paper's comparison with other review

papers by taking into account the following seventeen criteria: 1: IoT applications; 2: IoT components; 3: IoT architecture; 4: Attacks in IoT; 5: BCT types; 6: BCT characteristics; 7: DLT; 8: Evaluation criteria; 9: Consensus mechanism; 10: Smart contract; 11: Cryptocurrency; 12: Access control; 13: security enhancements in BC-based IoT; 14: IDS in BC-based IoT; 15: BC-based IoT Applications; 16: Challenges in IoT, BCT, and integration BC-based IoT; 17: Future research directions and open issues. While many researchers have studied BCT and IoT separately, few have explored the integration of BCT and IoT.

Our contributions can be summarized as follows:

- This survey provides an overview of the IoT, including its background, applications, components, architectures, and the various types of attacks to which IoT systems are vulnerable.
- This survey explores a state-of-the-art in BCT by highlighting its background, types, characteristics, relationship to DLTs, evaluation criteria, consensus mechanisms, smart contracts, cryptocurrencies, and access control techniques.
- This survey reviews the advantages of integrating BCT with IoT and recent research efforts on BC-based solutions to enhance IoT security and various BC-based IoT applications.
- Finally, in addition to highlighting the research challenges in IoT and BCT, as well as the challenges of integrating BCT with IoT, this work outlines several future research directions for open integration of BCT with IoT security, along with some solutions that researchers have proposed to overcome these challenges and limitations.

**Table 1. Criteria covered compared with other review papers.**

| Reference | Year | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| [9] | 2025 | ✓ | × | ✓ | ✓ | × | × | × | × | ✓ | × | × | ✓ | ✓ | × | ✓ | ✓ | ✓ |
| [10] | 2025 | ✓ | × | ✓ | × | ✓ | ✓ | × | × | ✓ | ✓ | × | ✓ | ✓ | × | ✓ | ✓ | ✓ |
| [11] | 2025 | ✓ | ✓ | × | × | ✓ | ✓ | × | × | ✓ | × | × | × | ✓ | × | × | ✓ | ✓ |
| [3] | 2024 | × | × | ✓ | ✓ | ✓ | ✓ | × | × | × | × | × | × | ✓ | × | ✓ | ✓ | ✓ |
| [4] | 2024 | × | ✓ | ✓ | ✓ | × | ✓ | × | × | × | × | × | ✓ | ✓ | × | ✓ | ✓ | ✓ |
| [12] | 2024 | × | × | × | × | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | × | × | ✓ | ✓ |
| [13] | 2024 | × | × | × | × | × | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ |
| [7] | 2023 | × | × | × | × | ✓ | ✓ | ✓ | × | × | ✓ | ✓ | ✓ | × | × | ✓ | ✓ | ✓ |
| [14] | 2023 | × | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ | × | × | ✓ | ✓ | × | ✓ | ✓ | ✓ |
| [15] | 2022 | × | × | × | × | × | × | × | × | ✓ | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | ✓ |
| [16] | 2021 | ✓ | ✓ | × | ✓ | ✓ | ✓ | × | × | ✓ | ✓ | × | ✓ | ✓ | × | ✓ | ✓ | ✓ |
| [17] | 2021 | × | × | × | × | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ |
| Our work | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

The remainder of our survey is structured as follows. Section II provides the background, applications, characteristics, architectures, and various types of attacks associated with the IoT. Section III presents a comprehensive overview of BCT. Section IV analyzes the integration of BC-based IoT. Section V reviews applications that leverage BC-based IoT. Section VI identifies challenges related to IoT, BC, and their integration, and discusses future research directions and open issues. Section VII presents the conclusion.

## 2. INTERNET OF THINGS OVERVIEW

This section offers a comprehensive overview of the IoT, including its applications and components. This section indicates many architectures proposed by researchers for the IoT. Moreover, this section discusses possible attacks in the IoT context. The term IoT first appeared in the 1970s, when British technology developer Kevin Ashton was working on Radio Frequency Identification (RFID) at Procter and Gamble [18]. The increasing accessibility of the Internet has improved global information exchange. At the same time, the IoT presents new options that can provide a competitive edge, covering wide domains from individual systems to multi-platform deployments and real-time cloud environments [19].

### 2.1. Internet of Things Applications

There are many applications (as shown in Figure 1) where IoT has been deployed. They have become intelligent and execute their tasks mechanically with assistance from the Internet [20]. The first application is healthcare, wherein sensors monitor human body temperature, blood pressure, and heart rate [21, 22]. Another application is smart cities, as individuals utilize several electronic devices such as refrigerators, microwave ovens, fans, heaters, and air conditioners within their residences. Installed sensors detect problems and relay them to the manufacturing company for resolution [22]. The third application of IoT is tracking animals. An animal's body embeds GPS sensors for efficient tracking. Animals also use it to monitor their nutrition [23]. Another IoT application is smart robotic grippers that directly engage with objects to gather sensory input. Numerous sensors and instruments, such as touch, motion, vision, optical, and force sensors, equip a smart gripper. The sensors equipped with a smart gripper determine their intelligence as they collect real-time information for decision-making. Consequently, they must adhere to design parameters, including cost, weight, and compactness [24].

Moreover, there are various IoT applications, including infrastructure management manufacturing, smart transportation, smart agriculture, smart retail, cryptocurrency, finance, reputation systems, copyright protection, energy, societal applications, advertising, mobile applications, defense, supply chain management, voting, agriculture, education, automotive, identity

management, asset tracking, law enforcement, digital records management, intrusion detection digital ownership management, property title registries, and other domains [15, 20].

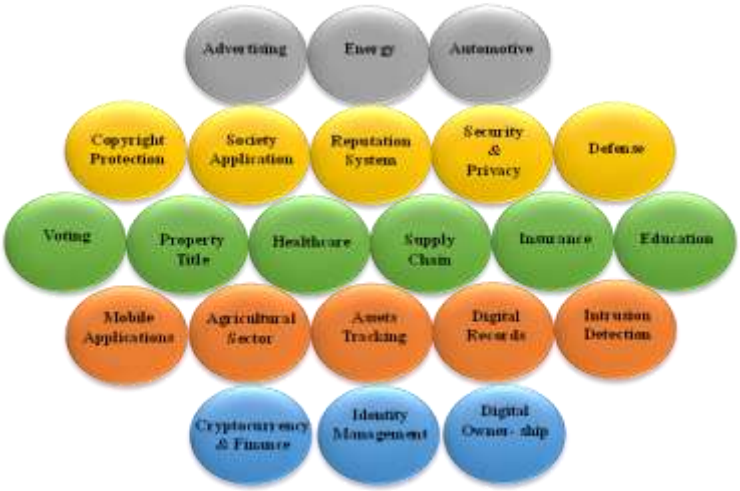


**Figure 1. Major IoT Applications in Various Industries [15, 25].**

### 2.2. Internet of Things Components

IoT offers numerous advantages and conveniences to users. Therefore, their proper utilization requires some components. This section discusses the components of IoT. Figure 2 illustrates the components required to provide IoT functionalities.

(1) Identification

Identification offers each object in the network a distinct identification. Naming and addressing are the two procedures involved in identification. While addressing indicates an object's specific location, naming indicates an object's designation. Although multiple objects may share the same name, each is always assigned a distinct address, distinguishing naming from addressing. Various methods, such as ubiquitous codes and Electronic Product Codes (EPC), enable object naming within a network [26].

(2) Sensing

Sensing is the process of collecting and storing information from environments or objects, using sensing devices such as wearable sensing for physiological data, RFID tags for tracking, actuators for movement control, and smart sensors for environmental monitoring [20, 27].

(3) Communication

Communication is a primary function of IoT, wherein many devices are interconnected and exchange information. Communication devices can receive and transmit files, messages, and other data. Many technologies are used to facilitate communication, including RFID [27], Bluetooth [28], Near Field Communication (NFC) [29], and Long Term Evolution (LTE), Wi-Fi [30, 31].

(4) Computation

Computation is executed on the information collected from the objects utilizing sensors. It is utilized to eliminate unnecessary and unnecessary information. Different software and hardware platforms have been developed to execute processing in IoT applications. Software platforms are significantly influenced by the operating system when processing tasks. Different operating systems are utilized, including Android, Lite OS, Contiki, Tiny OS, and MantisOS [32, 33]. However, hardware platforms utilized include Arduino [34], Raspberry Pi [35], and Intel Galileo [36].

(5) Services

Assistance IoT applications offer four distinct types of services. The first is an identity-related service, which is used to identify the objects that have transmitted the request. The service of information aggregation gathers data from numerous objects. The aggregation service also does the processing. The third service is a collaborative system that makes decisions based on the gathered information and transmits suitable replies to the devices. The final service is ubiquitous, designed to respond to devices immediately without constraints regarding time and location [20, 37].

(6) Semantics

IoT relies on semantics to help users fulfill their responsibilities. The fundamental function of IoT is to carry out its responsibilities. It acts as the central processing unit of the IoT. It collects all information and generates suitable decisions to transmit replies to the device [20, 38].


**Figure 2. Components of IoT System Architecture [20, 39].**

### 2.3. Internet of Things Architectures

There is no general agreement among researchers about the architecture of IoT [40]. Researchers have proposed various architectures, with the most common being the three-layer, four-layer, five-layer, and seven-layer architectures. Figure 3 illustrates these architectures.

(1) Three-layer Architecture

The three-layer architecture consists of three layers: the application layer, the network layer, and the perception layer. The applications of IoT include animal tracking, smart cities, smart homes, smart healthcare, etc. It is responsible for delivering services to the applications. Each application may have different services because they rely on the information that sensors collect. The application layer presents numerous challenges, with security becoming the most important one [41].

People often refer to the network layer as the transmission layer. It works as an interface between the perception layer and the application layer. It transmits and carries information collected through physical objects via sensors. The transmission medium can be either wired or wireless. It also assumes the role of interconnecting smart cities, network devices, and networks [33, 42].

The perception layer, also known as the sensor layer, functions similarly to human sensory systems, such as smell, vision, and hearing. Its primary role is to identify things and collect data from them. Various sensors, including 2-D barcodes, RFID tags, and others, are attached to objects to collect data according to the specific application's requirements [33, 43].

(2) Four-layer Architecture

The three-layer architecture, initially seen as a basic model, has limitations in addressing IoT's evolving needs. To overcome this, a four-layer architecture was proposed, retaining the original three layers while adding a support layer to enhance security. The support layer addresses security risks by verifying information transmission and safeguarding against potential threats [33, 44].

(3) Five-layer Architecture

The five-layer architecture builds on the four-layer model by adding two new layers: the business layer and the processing layer. This architecture addresses security and storage issues in IoT, and is considered capable of meeting IoT standards while securing IoT applications. The business layer manages application functions, while the processing layer handles data processing, reducing big data challenges [20].

(4) Seven-layer Architecture

The seven-layer architecture, primarily used by the IoT World Forum (IoTWF), offers a robust model for IoT systems [45]. It includes the following layers: Collaboration and Processes, Application, Data Abstraction, Data Accumulation, Fog (Edge) Computing, Connectivity, and Physical Devices and Controllers. Each layer plays a critical role in enhancing IoT functionality.

In the Collaboration and Processes layer, data combines from lower layers with commercial applications and facilitates user interaction with IoT devices, delivering economic value. The Application Layer acts as the interface for users to interact with IoT data, supporting applications like surveillance, optimization, and consumer behavior analysis. The Data Abstraction Layer filters and organizes data to create efficient, functional applications. The Data Accumulation Layer serves as an intermediate storage layer for incoming and outgoing data, using systems like SQL, Cassandra, and MongoDB. The Fog (Edge) Computing Layer optimizes data processing by reducing latency, enabling real-time decision-making through decentralized computing. The

Connectivity Layer extends connectivity to the cloud and ensures data transfer between physical and logical systems. The Physical Devices and Controllers Layer comprises IoT "things" like actuators, sensors, and edge nodes that establish connections between the physical and digital worlds [46]. Figure 3 illustrates the sequence of the three, four, five, and seven-layer architectures that have been proposed for the IoT.

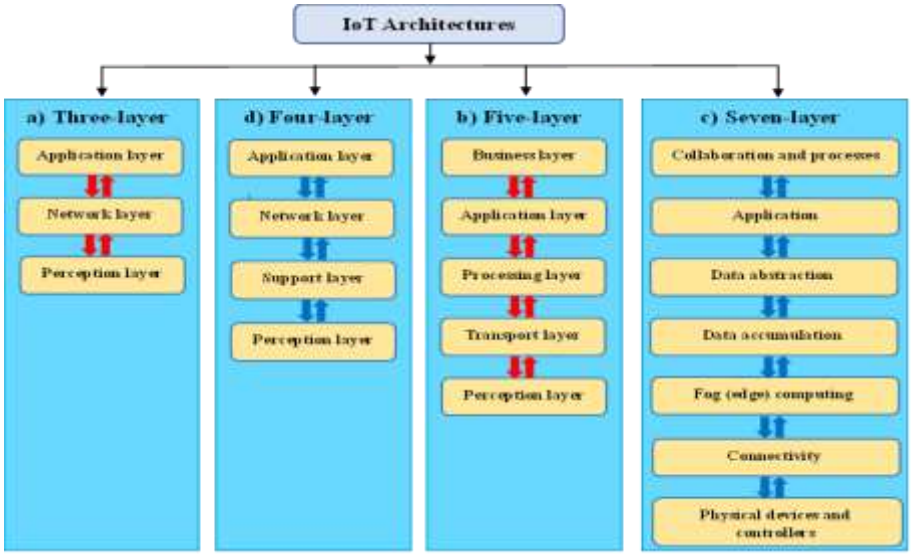


**Figure 3. Layered Models for IoT Architectures (3, 4, 5, 7 Layers) [20, 33, 47, 48].**

### 2.4. Types of Attacks in Internet Of Things

As the amount and variety of IoT devices grow, the attack surface increases greatly, rendering these systems more vulnerable to several security threats. Figure 4 depicts the grouping of IoT security attacks. Below is a brief overview of the types of attacks classified under four groups on IoT devices.

(1) Physical attacks

Physical attacks in IoT environments are adversarial actions that mainly target the wireless communication infrastructure, aiming to disrupt, degrade, or entirely block the reception and transmission of data packets between IoT devices and servers. Common examples of these attacks include eavesdropping, spoofing, jamming, and tampering. These attacks pose substantial risks to the reliability and security of critical IoT applications, including smart cities, innovative healthcare, and smart homes. Therefore, it is essential to include efficient detection and mitigation mechanisms, such as Automated Modulation Categorization (AMC), which enables suitable countermeasures and recognizes the modulation formats of the current attack [49].

(2) Software attacks

The proliferation and increased interconnectivity of IoT devices across various domains, such as smart cities, innovative healthcare, and smart homes have elevated the risk of software-based attacks that could compromise the privacy and security and of both users and systems. Software attacks targeting IoT can manifest in several forms, including malware, Denial-of-Service (DoS), spoofing, ransomware, and tampering. These attacks often exploit vulnerabilities in the software configuration, implementation, or design of IoT devices, as well as the networks through which they communicate. The repercussions of such attacks can be severe, leading to disrupted device functionality, theft of sensitive data, financial extortion, or even physical damage. Consequently, it is imperative to implement robust software engineering practices and security measures to effectively mitigate and prevent the risks associated with software attacks in IoT environments [1, 50].

(3) Network attacks

These attacks pose a considerable threat to the privacy and security of connected systems and devices. They can compromise the availability, functionality, integrity, and confidentiality of services and data provided by IoT devices. Common network attacks in IoT include Man-in-the-Middle (MITM), Denial-of-Service (DoS), replay, spoofing, and eavesdropping. To avoid or reduce these threats, many countermeasures can be applied across multiple layers of the IoT architecture, including authentication, firewalls, encryption, and intrusion detection [49, 51, 52].

(4) Application Attacks

Attacks against IoT applications primarily target IoT system services and user-facing interfaces. These interfaces, typically intended for data retrieval, interaction, or configuration, may serve as targets for attackers aiming for illegal access or harmful

alteration [51]. Phishing is a quintessential application attack. Phishing attacks use fraudulent methods to entice users into disclosing sensitive information, often by imitating authentic IoT application interfaces. SQL injection exploits programs' foundational databases, allowing attackers to insert harmful SQL instructions to obtain or alter data or unauthorized access. In web-connected IoT devices, cross-site scripting (XSS) enables attackers to embed malicious scripts into web pages, which are subsequently executed by unsuspecting users' browsers, potentially resulting in session breaches or data theft. Data leakage frequently arises from vulnerabilities or misconfigurations inside the program, unintentionally revealing sensitive information [53].

(5) Authentication and Authorization Attacks

Authentication and authorization are fundamental to IoT device security, ensuring the verification of user identities and the provision of appropriate access rights. As IoT ecosystems get more complex, these processes are increasingly exposed to targeting [51]. Attackers, identifying the opportunity to exploit vulnerabilities, infiltrate or seize control in these security checkpoints, resulting in illegal access and possible data compromise. Brute force attacks exemplify a direct yet persistent method wherein attackers' endeavor to obtain access by exhaustively testing all conceivable credential combinations until a successful match is achieved. Password cracking is utilizing known data or methods to ascertain or infer the right password, sometimes capitalizing on weak or frequently employed passwords. As one progresses from the initial access to subsequent sessions, session hijacking presents a significant concern. In this scenario, attackers hijack an active session between the user and the IoT device, circumventing the requirement for direct login credentials.

Finally, replay attacks involve malicious actors intercepting and retransmitting data, particularly authentication requests, to deceive IoT devices into providing access or executing undesired activities. Each of these assaults highlights the critical necessity for resilient and adaptive security protocols in the continuously growing domain of IoT [49, 51, 52].

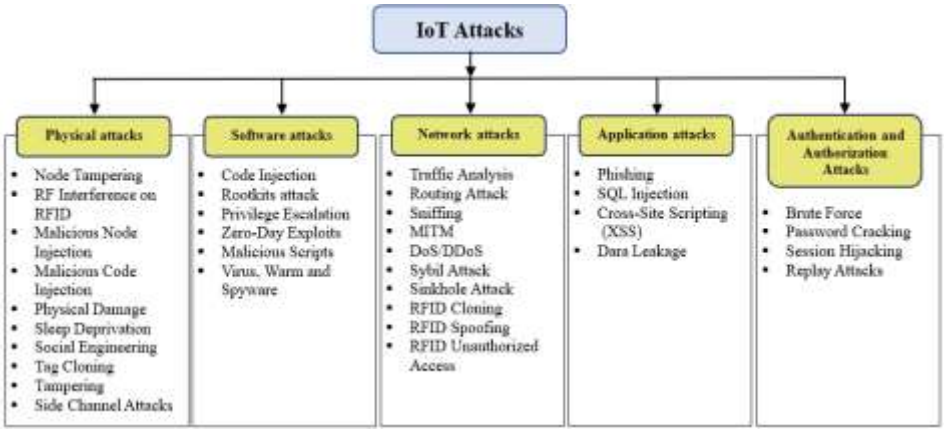


**Figure 4. Taxonomy of IoT security attacks [49, 51].**

## 3. BLOCKCHAIN OVERVIEW

This section presents a thorough analysis of BC, including an overview of different BCT types and an evaluation of significant DLT platforms using both quantitative and qualitative criteria. This analysis aims to aid DLT developers and architects in identifying the most appropriate platform that corresponds with their particular needs. This section also presents consensus mechanisms, smart contracts, and cryptocurrency. The characteristics of BCT and the associated challenges are also highlighted.

In 2008, a group of individuals, or a person known as Satoshi Nakamoto, published a groundbreaking paper on Bitcoin, describing a new decentralized, peer-to-peer electronic cash system [2, 8, 54]. The paper introduced BCT, a data structure for recording financial transactions, and explained the protocol that maintains the BC's validity across the network. Many people mix up BCT and Bitcoin. However, Bitcoin is a cryptocurrency that uses to allow it to trade freely and globally without the oversight of a central guarantor (banks). In other words, Bitcoin is essentially a financial application that utilizes BCT [17].

A BCT is characterized as a distributed ledger that is immutable, enduring, auditable, timestamped, and resistant to tampering. This ledger comprises a series of blocks that facilitate the storage and peer-to-peer (P2P) sharing of data [55]. Transaction histories, contracts, and personal data are just a few examples of the types of data that can be stored in a BCT [33]. At first, BCT appeared as a way to get around the double-spending problem that comes with cryptocurrencies [56]. Its adoption has surpassed the realm of cryptocurrencies due to its distinct and enticing features, which include enhanced security, transaction privacy, integrity, authorization capabilities, resistance to censorship, auditability, immutability of data, fault tolerance, and systemic transparency. As a result, BCT has been found to be applicable in a number of different sectors, such as supply chain management, intelligent transportation systems, agriculture, smart grids, mobile crowd sensing, Industry 4.0 implementations, identity management, and

the security of mission-critical systems [57, 58]. The significant focus on security, auditability, transparency, and anonymity has drawn a lot of interest in BCT from industry and academic sectors [13].

In BC, a public ledger is essential for recording digitally verified transactions of users in a peer-to-peer (P2P) system. This procedure utilizes asymmetric encryption to enable message decryption. A user generally possesses two cryptographic keys: a private key for decrypting received messages and a public key for encrypting messages meant for others. From the standpoint of BC, the private key is essential for the authorization of transactions on the BC. In contrast, the public key serves as an address or distinct identifier within the network. The procedural workflow begins with the user authenticating a transaction using their private key, followed by the dissemination of this signed transaction to their network peers [13]. These peers then confirm receipt of the signed transaction and distribute it throughout the network. Every node in the network keeps a copy of the ledger to improve transaction auditability. This ensures that any additions to the transaction record are confirmed and validated by other nodes, removing the need for centralized authority and preventing potential single points of failure. This distributed ledger is simultaneously updated and verified across all nodes [12]. The fundamental integrity of the BCT is protected by strong cryptographic methods that verify and connect blocks of transactions, making it extremely difficult to alter any individual transaction without detection [59]. The primary objective of BCT is to liberate individuals from the requisite trust in intermediaries, who presently dominate and oversee critical facets of societal functions [17].

In the operational framework of a BCT network, designated nodes known as miners are responsible for incorporating newly initiated transactions into a collective pool of transactions pending confirmation. The process persists until the total transactions attain a specified volume, known as the block size, at which point each miner aggregates these transactions into one block. The requirement to uphold a unified timeline of these blocks guarantees the uniformity of ledger copies across all entities and precludes the inclusion of transactions that are invalid, inconsistent, or contradictory, necessitating consensus among network participants. This consensus mechanism is crucial for preserving the BC's structural integrity and operational functionality, guaranteeing consensus on the ledger's current state among participants who may not possess intrinsic trust in each other [2]. Upon attaining a distributed consensus, miners proceed to incorporate a valid transaction into a timestamped block. This miner's inclusion is subsequently disseminated across the network. After validation and confirmation of alignment with the hash of its preceding block in the chain, this propagated block is subsequently attached to the BCT [60]. The methodology used to achieve consensus significantly affects the operational performance and security of the BCT network, underscoring the essential function of consensus mechanisms in enhancing the resilience and effectiveness of BCT systems [2].

### 3.1. Blockchain Technology Types

The conventional categorization of BCT into three primary types is based on permission prerequisites and data management methodologies [61]. Furthermore, a hybrid model exists that embodies a synthesis of public and private BCT systems [62]. Figure 5 illustrates this model, offering an overview of the various types of BC.

(1) Public or permissionless Blockchain

In a public or permissionless BC, entry into the network does not require permission, characterizing it as an open system that is accessible to the public without any centralized oversight. This type of BCT grants users unfettered access, ensuring that it remains independent of any single individual's or organization's ownership or control [63]. Within such a BC, every node in the network functions as an equal stakeholder, maintaining a complete record of all transactions. Public BCT facilitates universal participation in the verification and the consensus process of transactions. Notably, Bitcoin and Ethereum stand as quintessential examples of public BC. They utilize consensus protocols such as Delegated Proof of Stake (DPoS), Proof of Stake (PoS), and Proof of Work (PoW) to ensure network integrity [64].

(2) Private or permissioned Blockchain

A private or permissioned BCT restricts access to only those users who have been expressly authorized. This architecture establishes a closed and secure environment, yielding enhanced levels of security and privacy compared to its public counterparts [63]. The governance of the network is typically centralized and vested in either a single entity or a select group of authorities. Private BCT are particularly advantageous when privacy and security are paramount, permitting only certain nodes and users to execute transactions. These BCT are lauded for their emphasis on speed, scalability, and security, making them ideally suited for applications in supply chain management and the facilitation of transactions between companies within a federated context. Among the consensus protocols utilized in private BCT are Practical Byzantine Fault Tolerance (PBFT), Proof of Elapsed Time (PoET), and Proof of Authority (PoA) [64].

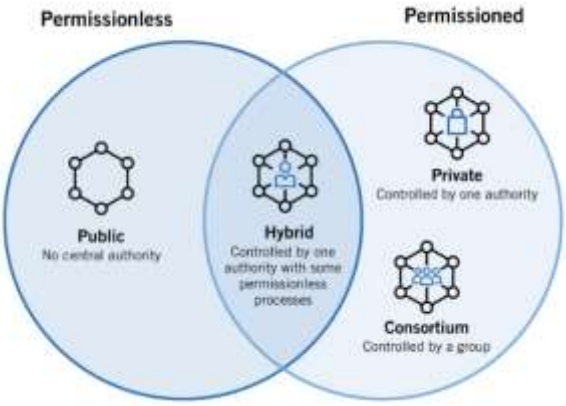


**Figure 5. Various types of BCT [65, 66].**

(3) Consortium Blockchain

This variant of BCT is collectively managed and operated by a consortium consisting of multiple organizations or entities. In a consortium BC, only a select group of peers participates in the consensus process. This setup is partially decentralized, and read access can be either open or restricted to specific peers. A small, selected group confirms the validity of the blocks [56, 67]. It proves especially advantageous in scenarios where several organizations seek to collaborate yet wish to maintain specific degrees of privacy and control. Furthermore, consensus protocols such as PBFT, PoT, and PoV are employed to ensure the efficiency and integrity of the network [64].

(4) Hybrid Blockchain

The hybrid BCT model amalgamates the most advantageous features of both public and private BCT. It facilitates private transactions within a network that is interconnected with a public BC, thereby enhancing safety and transparency [68]. Interaction within the network is mediated through smart contracts [69], facilitating a framework that permits the selective dissemination of information while capitalizing on the decentralized aspect of the public BC. Despite this controlled environment, the BCT retains its immutability, rendering alterations or deletions infeasible. The network's operations are governed by automated smart contracts, with roles and permissions being explicitly predefined. It has several advantages over traditional BCT [8, 70]. In Hybrid BC, the primary benefit is maximum customization, which combines the advantages of private, permission-based systems and public, permissionless systems. Hybrid BCT is flexible enough to allow users to join easily, similar to private BC. This type of BCT is able to enhance the transparency and security of the BCT network [8, 71, 72]. Table 2 presents a comprehensive summary of the different types of BC.

**Table 2. Comparison of various types of BCT [8, 17, 66, 73].**

| Feature | Public | Private | Hybrid | Consortium |
|---|---|---|---|---|
| Access | Anyone can join | Restricted access | Selected public and private aspects | Limited to consortium members |
| Permissioned/ Permissionless | Permissionless | Permissioned | Permissioned and Permissionless | Permissioned |
| Level of Centralization | Fully decentralized. | Highly centralized. | Mixture of both, depending on the configuration. | Partially decentralized. |
| Consensus Mechanism | PoW, and PoS. | PBFT, and PoA. | Can incorporate different mechanisms for different sectors. | PBFT, PoA, or other agreed mechanisms by consortium members. |
| Advantages | Decentralization, transparency, security | Privacy, speed, control | Flexibility, the combination of privacy and transparency | Shared control, efficiency, privacy balance |
| Disadvantages | Slower transaction times, scalability issues | Less decentralized, limited transparency | Complexity in design and maintenance | Requires trust among consortium members |

BCT comprises a series of sequential blocks, each capable of storing a variety of transactions. The initial block mined within a BCT is referred to as the Genesis Block. Every block within the BCT is composed of two primary sections [17], as illustrated in Figure 6. The first section, known as the header, encompasses critical information pertaining to the block itself. This block header typically includes: 1) the block version; Mark the block protocol version (indicates the position of this block in the BC). 2) the previous block hash; A hash value linking the block to the previous block. To generate block hashes, the BCT uses the SHA256 hashing algorithm. 3) Merkle tree root: It is the hash value of all the transactions included in the current block. Thus, transactions

cannot be changed without changing the Merkle root hash. One modification in one block payload will change the Merkle root hash value, which invalidates the block. 4) timestamp: The time in which this block is generated. 5) difficulty (D); The difficulty target of the proof-of-work calculation for generating this block (it is a measure of finding a successful hash). 6) nonce (N). It is a counter used in the PoW and usually starts with 0 and increases for each hash computation. Simultaneously, this prevents reboot attacks. Number of transactions recorded in this block. 7) byte; Size of this block in byte ( excluding this field) [74].

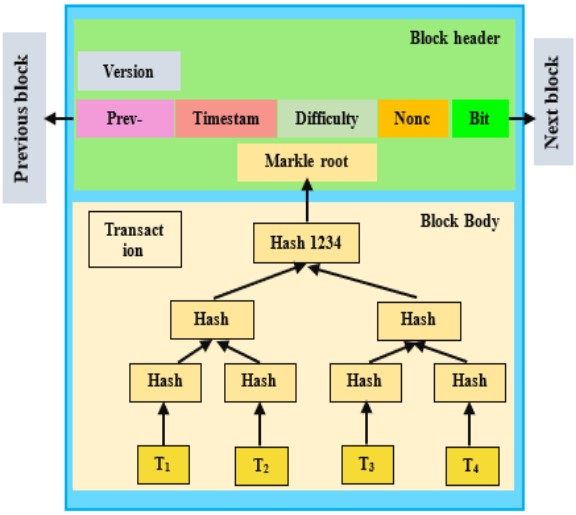


**Figure 6. Block structure [17, 73].**

The second component termed the body, encapsulates the transactions or records (which the database is intended to store) and can encompass a diverse array of data types, including but not limited to monetary transactions, traffic information, health data, and system logs. The body of the block meticulously records all inputs and outputs associated with each transaction. Inputs integrate the outputs from preceding transactions along with a signature field authenticated by the owner's private key, serving as evidence of asset ownership. Conversely, outputs detail the assets to be transferred and the recipient's address (corresponding to the recipient's public key). This design ensures that only the recipient, possessing the matching private key, can expend the asset, thereby establishing a secure mechanism for asset transfer and ownership verification [74, 75]. The distributed and append-only nature of BCT improves transaction security and integrity [6, 67, 76]. The BC's chaining method (shown in Figure 7) ensures immutability by incorporating the hash of the previous block into the current block. Indeed, if a malicious user wants to change or modify a transaction on a block, he/she must change all following blocks as well because they are linked with their hashes. Then, he/she must update the BCT version on each participating node [17, 67, 75, 77].

### 3.2. Blockchain Technology Characteristics

BCT is characterized by several properties, as follows. Figure 8 provides the basic properties of BCT.

(1) Distributed

It is crucial to recognize that a decentralized ledger is essential to this innovation since BCT is a subset of DLT. Every node in the network that is involved receives a copy of this ledger, so every node is in possession of the same copy [78]. As a result, each node in the network has access to and can examine the entire transaction history. The fact that this access is provided without the requirement for a centralized authority emphasizes even more how decentralized BCT is [7, 79].

(2) Decentralization

In traditionally centralized architectures, a central authority or intermediary manages the validation and oversight of transactions. Conversely, transactions are validated and authenticated via a decentralized network of nodes in BCT. Transactions are disseminated to each network node at the commencement of the process. To validate a transaction in a decentralized manner, rather than relying on a central authority, each node can mine a new block containing the transaction. Furthermore, the principle of decentralization diminishes the likelihood of a single point of failure, guaranteeing that services remain operational even if certain nodes are inaccessible [7, 8].

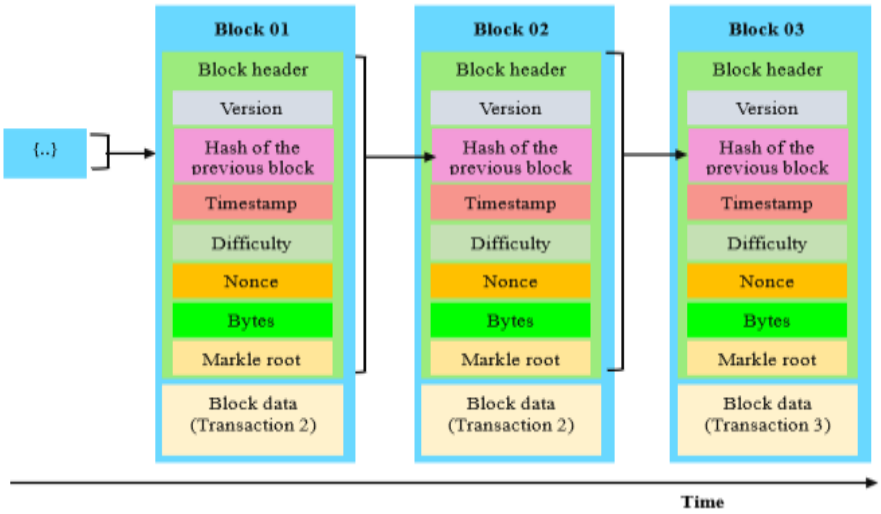


**Figure 7. BCT structure [17, 73].**

(3) Immutability

All data, including blocks and their associated transactions, are secured and interlinked through cryptographic methods. A slight change in any transaction within a particular block result in a substantial modification of the Merkle root hash, thereby affecting the hash value of the block's header. This chain reaction requires significant recomputation and agreement among the involved nodes to alter all subsequent blocks. As a result, once a block is mined and integrated into the BC, it is considered immutable or tamper-resistant [8, 80].

(4) Provenance

The decentralized nature of BCT is reflected in the distribution of transaction details across all nodes whenever a transaction is recorded on the BC. Furthermore, BCT uses timestamps in every transaction so that all nodes can keep track of the transactions in chronological order [81]. Users have the ability to confirm and follow transactions at any point in time because every transaction is permanently and transparently recorded across all nodes [82]. This feature guarantees the data's transparency and traceability [83].

(5) Availability

This represents a critical attribute of BCT, signifying that services remain perpetually accessible to users owing to the decentralized architecture of the BCT network. Consequently, this framework renders the system resilient to a myriad of disruptions, whether they are deliberate, such as denial-of-service attacks, or occur inadvertently [67].

(6) Transparency

One other essential component of BCT is transparency. Every node in the network has access to comprehensive data about transactions and the values they are linked with. Due to its copy of the ledger, every node in the distributed network has the ability to confirm and track past records. This feature supports the ideas of immutability and verifiability, improves data sharing, and builds a trusted workflow [81, 84].

(7) Anonymity

An additional noteworthy benefit of BCT is its anonymity. BCT generates a distinct alphanumeric address for each user, ensuring their pseudonymous anonymity within the BCT network. This configuration ensures that a central body does not supervise users' personal data. Between these BC-generated addresses, transactions are enabled, providing a certain level of privacy. It is important to note, however, that although this feature improves privacy, it may unintentionally encourage illegal activity [83, 85].

(8) Non-repudiation

For BCT, non-repudiation is an essential component. This principle guarantees that users who apply cryptographic techniques, such as digital signatures, cannot retract their actions within the system [67, 86].

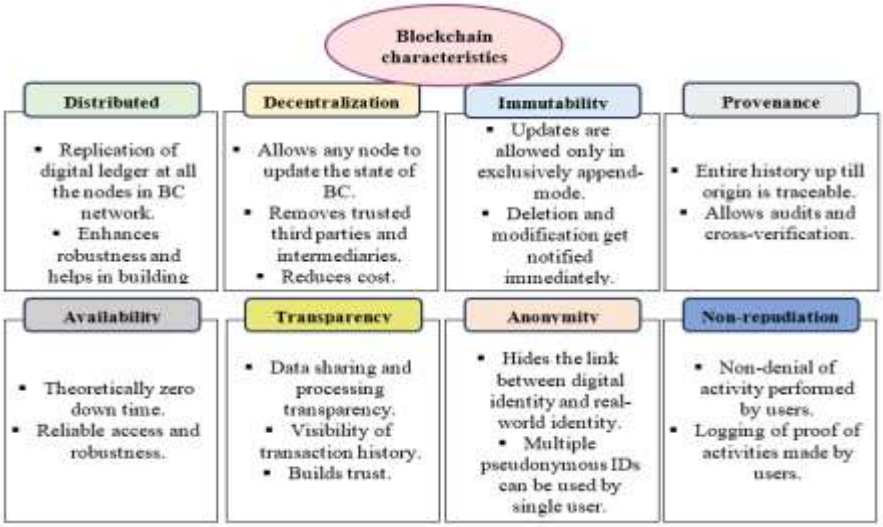


**Figure 8. Basic Characteristics of BCT [7, 78-80].**

### 3.3. Distributed Ledger Technology

This subsection evaluates the feasibility of several DLT platforms: Bitcoin [6], Ethereum [87], Hyperledger [88], Multichain [89], IOTA [90], and Corda [91]. These platforms were selected based on quantitative criteria, including scalability, latency, and throughput, as well as qualitative factors such as governance structure, security features, and their suitability for various use cases. They represent the most established options in both private and public distributed ledgers, supporting a variety of applications from basic IoT scenarios to complex financial systems.

There are numerous BCT platforms available for various purposes. Bitcoin is a digital payment and cryptocurrency system launched in 2008 [6] on a peer-to-peer network by Satoshi Nakamotov, [67]. It uses pseudonyms and operates via transactions, consensus protocols, and communication networks. A conflict occurs when multiple miners generate blocks simultaneously, with each considering its block as legitimate. To prevent conflicts, Bitcoin uses the longest chain rule, which ensures the integrity of the BCT and prevents conflicts between miners sharing the same BC.

In 2013, Ethereum was introduced as a public BCT platform that uses smart contracts to write and execute code distributed [87]. It is a programmable BC, allowing users to create complex operations beyond Bitcoin transactions. Ethereum's core is the Ethereum Virtual Machine (EVM), which isolates code from network access, processes, or filesystems. To validate blocks, Ethereum uses a PoW mechanism called Ethash. A beta version uses a PoS-based protocol called Casper. Ethereum can also be used as a private BCT with pre-selected nodes, eliminating the need for a proof-of-work mechanism. However, Ethereum has faced security issues, including the 2016 DAO hack [92]. A DAO, a smart contract-based entity, was compromised by an attacker who exploited a bug to drain 3.6 million ETH (equivalent to $70 million). The attacker could request the ether's return multiple times before updating the smart contract's balance. The DAO's young language and limited support made modifications difficult [93].

Hyperledger is an open BCT platform launched in December 2015 by the Linux Foundation [94]. Its key purpose is to enhance the performance and reliability of the ledger. The platform prompts collaboration across various industries to advance BCT. The Linux Foundation provides a modular framework that supports various components for various uses, fostering a collaborative environment for the development of enterprise BCT solutions. The combination and interaction of these components contribute to the platform's success [95]. Since 2015, the Hyperledger project has seen significant advancements thanks to cooperation with organizations such as the Enterprise Ethereum Alliance (EEA), Microsoft's Coco, and Cisco leading to the development of various Hyperledger platforms, including Sawtooth [96], Iroha [94], Indy [97], Fabric [98], Burrow [97], and Besu [99]. Figure 9 illustrates the various platforms and tools available within the Hyperledger project.


**Figure 9. Hyperledger Enterprise BCT [95].**

The Intel team developed Sawtooth Hyperledger, which is a platform used for developing, deploying, and implementing distributed ledgers. It features a consensus algorithm based on network size, including PoET, enhancing scalability. The platform supports permissioned and permissionless deployments, offering versatility [100].

Hyperledger Iroha, developed by Soramitsu, NTT Data, Colu, and Hitachi, aims to simplify integration of distributed ledger technologies into projects [116]. It focuses on mobile application development with client libraries for Android and iOS, and is highly preferred by C++ language developers [94].

Hyperledger Indy developed by the Sovrin Foundation, offers numerous identity management tools to developers and solutions architects [97]. Hyperledger Fabric is an open-source, permissioned BCT framework tailored for industrial use cases [100]. Hyperledger Fabric is a framework that can work on different operating systems [101]. According to Rasti and Gheibi, Hyperledger Fabric is a revolutionary framework with membership services and plug-and-play properties for BCT solutions [98]. Monax developed Hyperledger Burrow and allows developers and architects to create an EVM environment within Fabric and Sawtooth networks, leveraging Ethereum functionality in conjunction with Hyperledger functionality [97].

Hyperledger Besu is an open-source Ethereum client written in Java that utilizes the Ethereum public network. Additionally, it is the most recent project to join the Hyperledger platform [99]. Hyperledger tools are software used to manage and execute BCs, monitor and explore ledger information, and design and improve BCT networks [102-104].

The main tools associated with Hyperledger [105, 106] include Avalon [14], Composer [91], Cello [91], Explorer [107], and Caliper [91]. Table 3 displays a comparison between platforms under the Hyperledger project.

**Table 3. Difference between Hyperledger platforms [101, 103, 108].**

| Property | Sawtooth | Iroha | Indy | Fabric | Burrow | Besu |
|---|---|---|---|---|---|---|
| Hosted by | Linux foundation | Linux foundation | Linux foundation | Linux foundation | Linux foundation | EEA |
| Advantages | Distributed state agreement, Adapters for transaction logic, Versatility, Scalability, Transaction families | Mobile libraries | Identity management | Enterprise backing, Relative maturity, Private channels, Modular architecture, Smart contracts | Lower barrier to entry, Use of the EVM | Mobile libraries |
| Smart contract technology | Transaction Families | Chaincode | None | Chaincode | Smart contract application engine | Three types of transactions |
| storage | Central lmdb database | Kura | RocksDB | CouchDB or leveldb | Google's Protocol Buffers | RocksDB |
| Smart contract language | C++, Java, JavaScript, Go, Python, Rust, or Solidity | Java, JavaScript, Swift, or Python | C++, Java, JavaScript, Python, Swift, Rust | Go, Solidit, Java, Javascript | Solidity or Wasm | Java or Solidity |
| Status | Active | Active | Incubation | Active | Incubation | Not Available |
| Consensus Algorithm | PoET, PBFT, Raft, Devmode | BFAT called sumeragi | RBFT | Any consensus can be plugged, including Raft, Kafka, Solo | PoS protocol called tendermint | PoA (IBFT 2.0, Clique and Etherhash, and PoW |
| Cryptography | SECP256K1 ECSA | ED25519/SHA512 | ED25519 | ECDSA and SHA256 (abstracted) | ED25519/SHA512 | Not Available |
| Types of Consensus Algorithm | 1.Poet -Lottery Based 2.poet simulator voting based 3.RAFT-voting based | Voting Based | Voting Based | Application Dependent | Voting Based | Voting Based |

Multichain is an open-source platform that enables the creation and deployment of private distributed ledger applications originating from Bitcoin BC. It allows end users to configure block size, target time for blocks, active permission type, mining diversity, mining reward, chain protocol, permitted transaction type, and metadata [109]. Multichain provides a simple API and command line interface for maintaining and deploying DLT systems. It covers various use-cases such as connected health, KYC, insurance security, and the food supply chain. Multichain solves problems related to mining, privacy, and openness through integrated management of user permissions. The platform implements a hand-shaking process, requiring nodes to present their identity as a public address on the permitted list and verify that the other's address is on its own permitted list. Unlike Bitcoin, Multichain uses a distributed consensus among identified validators to restrict mining to a set of identifiable entities. It also uses a randomized round-robin system for block adders to ensure a fair mining policy. Transaction fees and block rewards are set to zero by default, but users can configure parameters as needed. Multichain 2.0 Beta, released last year, offers smart contract support for custom rules regarding transaction or stream item validity [110, 111].

IOTA is a distributed ledger designed for the IoT that offers secure communications and payments between devices [90]. It uses Tangle, a consensus-building data structure made of a Directed Acyclic Graph (DAG), to solve the double-spending problem and scalability issues faced by most distributed ledgers, including Bitcoin [112]. IOTA turns users into miners by requiring them to approve two transactions before verifying transactions. There are no dedicated miners, but those making transactions are the actors affecting the system. Tangle uses an orderly approach to verifying transactions to reach consensus, ensuring that each network member must verify two other transactions before verifying their own. This makes the IOTA network more distributed than a BCT network, as it is distributed among every participating node. IOTA's scalability, fast transactions, and ability to validate an unlimited number of transactions simultaneously make it suitable for IoT device use cases. IOTA plans to introduce Qubic, a smart contract capable of providing general-purpose, cloud, or fog-based permissionless multiprocessing on Tangle [111].

Corda is a DLT designed for finance use-cases. It is a permissioned network with verifiable identities using public-key infrastructure [91]. Corda differs from mainstream platforms like Bitcoin and Ethereum in that it does not use a BCT for recording transactions. Instead, it aims to make entities aware of transactions directly involved, reducing privacy dilution. For example, a bank can only disclose transactions involving a customer owed a certain amount to the bank, the customer, and relevant regulatory organizations. Corda is a distributed ledger that uses consumable states to operate transactions, eliminating the need for block-styled architecture. It operates on consumable states, which are analogous to the latest entry of a BCT ledger. Consumable states are used to validate new transactions, and the consensus is reached at the transaction level by involving relevant parties only. Validity is secured by checking for all required signatures and ensuring that any referred transactions are also valid. Uniqueness concerns the input states of a transaction, ensuring that the transaction in question is the unique consumer of all its input states. Corda stands out from renowned financial networks like Ripple and Stellar due to its smart contract facilities. It acts as both a financial network and a platform, combining the best of Ethereum/Hyperledger and Ripple/Stellar domains. Corda has a large developer community that can write Java and Kotlin code to develop DApps in the platform [111, 113]. There are some other BCT platforms, in addition to the previously discussed platforms, such as Ripple [114], HDAC [115], Cosmos [116], IoTeX [117], BigchainDB [118], ChainCore [75], Domus Tower BCT [119], HydraChain [120], OpenChain [121], EOS [122], Cardano [107], and Waltonchain [102]. The comparison of the selected platforms using the quantitative and qualitative criteria is presented in Table 4.

### 3.4. Evaluation Criteria

The evaluation of DLT platforms necessitates a nuanced approach that incorporates both quantitative and qualitative criteria (as shown in Figure 10) to provide a holistic understanding of their capabilities and performance. These criteria are essential for stakeholders, including developers, architects, and researchers, to assess the suitability of various DLT platforms for specific applications. Below, we delve into each category and the relevant criteria that underpin the comprehensive evaluation of DLT platforms.

Within the scope of [38] paper, quantitative criteria are categorized as those with quantifiable properties or objective assessment, and each of these criteria is discussed in detail. Type refers to the type of ledger the specific system utilizes. Cost the deployment and use of an existing DLT design incurs hardware, energy, servicing, and maintenance costs, including network-based services. Transaction fees, also known as transaction fees, can be reduced as no human involvement is involved, thereby reducing the overall cost of deploying and using network-based services [123]. Scalability refers to a system's ability to process large amounts of data within a specific timeframe. A highly scalable system is more adaptable to various scenarios and is determined by the combination of block size and block creation time. The consensus algorithm is a crucial component in achieving distributed consensus in the DLT system, directly influencing block creation time and energy consumption. Privacy analysis evaluates the privacy mechanism of any DLT system, revealing that a system with a built-in privacy-preserving feature is more likely to be widely adopted. Identity and Auditability can be utilized to analyze the identification of each entity and its impact on auditability. Suitability refers to a system's ability to support various data types, sizes, and/or volumes, enhancing its chances of large-scale

adoption. Robustness and Resilience is a critical analysis that assesses a system's ability to withstand various types of attacks and unprecedented errors.

**Table 4. BCT platforms comparison [17, 111].**

| Criteria | Bitcoin | Ethereum | Hyperledger Fabric | Multichain | IoTA | Corda |
|---|---|---|---|---|---|---|
| Type | Public | Public | Private | Private | Private | Private |
| Energy | High | High | Very low | Very low | Very low | Very low |
| Permission ? | No | Yes | Yes | Yes | Resemple in work | Yes |
| Permissionless? | Yes | Yes | No | No | Yes | No |
| Cryptocurrency | Bitcoin | Ethereum | No native cryptocurrency | Multi-Cryptocurrency | mIoTA | Corda does not have its own cryptocurrency |
| Block size | 1MB | Ethereum's block size varies (implicit restriction) | Configurable | Configurable | Configurable | Configurable |
| Block time | 10m | 15sec | 0.5-2 sec | Configurable | Configurable | 0.5-2 sec |
| Consensus | PoW | PoW, PoS | PBFT | Round robin | Tangle | Notaries |
| Privacy | Transactions, linked by pseudonymous identifiers, are publicly visible. | Transactions, including smart contracts, are publicly linked by pseudonymous identifiers. | The private ledger ensures user privacy via channels that keep interactions confidential among selected network peers. | Privacy management through controlled user permissions. | Pseudonymous | Privacy enhancement via unified user permission management. |
| Identity and Auditability | Identification through public keys enables auditability and accountability in a public ledger, contingent on authenticating entity identities. | Public keys provide pseudonymous identification in a public ledger, bolstering auditability and accountability when identities are verifiable. | PKI-based identification mandates entity registration and key issuance, enhancing auditability and accountability. | Public key cryptography enables verifiable identities, supporting auditability and accountability. | Pseudonymous | Pubic Key Infrastructure |
| Suitability | OP_RETURN opcode supports storing small data (about 80 bytes) but lacks smart contract processing capabilities. | Allows storing large data volumes at potentially high costs and supports smart contracts for immutable on-chain data processing. | Enables storing large data volumes and supports smart contracts for on-chain data processing. | Allows storing large data volumes (up to 1GB per item off-chain) and Version 2 introduces smart contracts for custom transaction or data validation rules. | Suitable for IOT data | Financial data |
| Robustness and Resilience | Robust P2P network with enhanced immutability and resilience, driven by consensus algorithms and broad adoption. | Robust P2P network, ensuring data and code immutability through consensus algorithms and broad adoption. | Strong P2P network resilience tied to the count of endorsers and orderers. | Robust P2P network with advanced data support, resilience varies with validator numbers. | Strong P2P framework with many orders. | Strong P2P network with resilience tied to validator count. |
| Trust level | High | High | Emerging | Moderate | Moderate | High |
| Governance | Bitcoin enhancements are proposed through BIPs, maintained by developers, and require consensus from users and miners for adoption. | Ethereum updates via EIPs rely on developer efforts and consensus from users and miners for off-chain features and on-chain governance. | The open-source codebase, under the Hyperledger Foundation charter and maintained by a committee, permits universal development participation. | The codebase, governed by Coin Sciences Ltd and maintained by the Multichain Development Team, is being upgraded with enterprise-level features. | The open-source codebase is regulated by the IOTA Foundation and upheld by the IOTA Development Team. | Managed by R3, the codebase is periodically updated, with V4.1 being the latest release. |
| Upgradability | Upgrade Of ledger is carried out via soft and hard fork. | Upgrade Of ledger is carried out via soft and hard fork smart contract is not upgradable. | Core software upgrades are executed by Fabric committee members, while chaincode updates utilize the version property. | Upgrade of the core software is carried out by the Multichain development team. | Upgrade of the core software is carried out by the IOTA development team. | Ledger upgrades occur via soft and hard forks; smart contract upgradeability is yet to be determined. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Sustainability | The sustainability of the PoW algorithm's energy use is doubtful, lacking a clear solution. | The future sustainability of the PoW algorithm's energy use is in doubt; a shift to a hybrid PoW/PoS solution is proposed for sustainability. | Sustainability relies on Fabric committee members' commitment in the Hyperledger Foundation and organizations' adoption for various use cases. | Multichain's sustainability is tied to client satisfaction, evidenced by its 86 company partnerships. | Exceptionally sustainable, as each participating node requires energy for validating only two transactions to confirm a transaction. | Corda's sustainability depends on its use by clients, with around 300 companies applying it in finance. |

In the absence of a measurable objective argument, subjective arguments are classified into quantitative categories, with each criterion corresponding to this property being described below. Trust level DLTs enhance trust by ensuring immutable record-keeping in the block, enabling data verification through multiple nodes. Governance is the governance mechanism of a DLT system, highlighting that a democratic and open system can boost public confidence, ultimately enhancing the trust level. Upgradability is a desirable feature that allows for the addition of new features or the correction of system errors, ensuring seamless integration and backward compatibility. Sustainability is the long-term sustainability of a system's ecosystem, crucial for its continuous wide-scale adoption [111, 124].


**Figure 10. Evaluation criteria for DLT Platforms [111, 124].**

### 3.5. Consensus Mechanism

Consensus protocols are a crucial element of BCT. They help a distributed network of nodes reach an agreement on the state of the BCT without relying on a central intermediary or authority. These protocols ensure that all nodes in the network maintain a consistent copy of the BCT and protect against malicious actors who tamper with the data. Several consensus protocols are used in BC, including PoW, PoS, and DPoS [125]. The integration of BCT within the IoT paradigm could yield numerous advantages, including the enhancement of data trustworthiness and the assurance of non-repudiation. IoT sensors, on the other hand, have fundamental problems because they can't handle the high computational needs of BCT. This is because IoT sensors have limited computational capabilities. A simplistic implementation of BCT in the context of IoT may consequently lead to protracted delays and an excessive consumption of computational resources [126]. The attainment of consensus by a majority of the peers for each block is paramount for the BC. Nevertheless, within extensive systems, these prerequisites precipitate a diminution in the transaction velocity as the duration required to achieve consensus augments exponentially. Modern commercial BCT frameworks, like Hyperledger, have tried to get around this problem by limiting the number of peers that can participate and only verifying transactions. Because there is no longer any block verification and Byzantine Fault Tolerance is not required, these changes might make it easier for bad transactions to happen [127]. Many researchers have proposed consensus mechanisms for BC-IOT. Table 5 presents a brief description of the consensus mechanisms discussed previously.

### 3.6. Smart Contract

An executable code on a BCT, known as a smart contract, executes when specific conditions meet certain requirements. Only the incorporation of associated transactions into a new block initiates these contracts, eliminating non-determinism that could otherwise affect the outcome of executions [128]. Nick Szabo coined the term "smart contract" in 1993, characterizing it as a computerized transaction protocol that executes the terms of a contract. While Bitcoin introduced a basic scripting language for this purpose, its limitations necessitated the development of new BCT platforms equipped with comprehensive smart contract functionalities [129].

Smart contracts significantly augment the autonomy of IoT devices by empowering them to verify if agreements meet contractual stipulations autonomously. By facilitating the elimination of regulatory overheads and acting as a ledger to affirm transaction completion, smart contracts enhance operational efficiencies. In the context of BC-enabled IoT ecosystems, they enable devices to document and authenticate transactions prior to their activation. Smart contracts in this architecture execute business logic automatically, protecting the system's core mechanism from threats like denial-of-service (DoS) attacks [130]. Smart contracts execute business logic automatically in this architecture, protecting the system's core mechanism from threats like denial-of-service (DoS) attacks [130]. Smart contracts thus foster a high level of collaboration and cohesion in managing

transactions and interactions. Therefore, smart contracts enable the ledger's service to incorporate the language of transaction terms and the necessary calculations to ensure their fulfillment. This improves the application's overall performance by making it easier to keep records and make sure transactions are valid [105].

Ethereum stands out as a leading BCT platform that supports the extensive use of smart contracts, facilitating a broader application scope beyond mere cryptocurrency exchanges [54]. Platforms such as Hyperledger demonstrate this capability by deploying smart contracts across the network in packages known as chain code [87]. These contracts allow the verification of assets in a variety of transactions, including those involving non-monetary items. This demonstrates the potential of smart contracts to broaden the scope of BCT [129].

**Table 5. Consensus mechanisms for BC-IoT.**

| Paper | Year | Name of algorithm | Outcomes |
|---|---|---|---|
| [131] | 2025 | Reputation-based Hybrid Consensus Mechanism (RepuICN) | ▪ RepuICN reduces block broadcast latency by 17% for regular blocks and 61.4% for checkpoint blocks, improving consensus efficiency.<br>▪ Achieves 3.4 times higher transaction throughput compared to Casper FFG under identical network conditions.<br>▪ Reduces network bandwidth consumption and enhances stability, particularly when handling network latency fluctuations. |
| [132] | 2025 | Fog-based BCT architecture | ▪ The fog-based BCT system efficiently manages an increasing number of IoT devices and transactions.<br>▪ The integration of the PoA and DPoS consensus mechanisms significantly reduces energy consumption compared to traditional consensus mechanisms. |
| [133] | 2024 | BC-enabled Lightweight IDS (BL-IDS) | ▪ BL-IDS focusing on addressing security challenges inherent to the decentralized and infrastructure-less nature of MANETs.<br>▪ A hybrid authentication mechanism is developed for node verification, formation of secure clusters based on similarity indices for efficient communication, and optimization of routing via the wild horse optimization algorithm. |
| [134] | 2024 | - | ▪ Addressed the security issues of IoMT devices, such as inadequate computation and storage, by proposing a novel group authentication scheme that reduces latency and improves throughput for authenticating IoMT devices.<br>▪ Security analysis confirmed the framework resistance to authentication-related attacks, supporting the scalability of IoMT systems. |
| [135] | 2024 | Proof-of-Light (PoL) | ▪ low-powered signcryption scheme and a novel consensus mechanism is developed, Proof-of-Light (PoL), aims at improving transaction throughput and reducing mining overheads.<br>▪ Demonstrated the scheme resilience and practical applicability in IIoT settings. |
| [136] | 2024 | Federated Distillation and BCT empowered Secure Knowledge Sharing (FDBC-SKS) | ▪ FDBC-SKS enables secure, decentralized knowledge sharing by combining federated distillation with a BCT consensus mechanism, enhancing model flexibility and reducing communication overhead.<br>▪ Outperformed existing methods in learning efficiency and consensus speed, as demonstrated in experiments using real-world datasets.<br>▪ Ensured data privacy and security, offering a scalable solution for IoMT applications. |
| [137] | 2024 | A random quantum Proof of Authority (RQPoA) | ▪ Enhanced decentralization by using a Verifiable Delay Function (VDF) for fair leader node election.<br>▪ Improved system availability by sharing the leader node's identity among validator nodes through a multi-party quantum secret sharing protocol, eliminating a Single Point of Failure (SPOF).<br>▪ Enhanced robustness and fault tolerance by adopting a quantum threshold signature for block voting, making it more secure against quantum computing threats. |
| [138] | 2023 | DPOS-PBFT | ▪ Maintain a messaging success rate of approximately 97% even after 3,000 user requests.<br>▪ Kept the maximum delay below 8 seconds, with an average delay of 2.38 seconds after 3000 requests.<br>▪ It showed superior overall performance compared to traditional consensus mechanisms (Raft, POW, POS, DPOS, PBFT).<br>▪ Provided minimal impact on system hardware efficiency, with less memory and disk space usage.<br>▪ Demonstrated significant improvements in the efficiency of storage and message transmission within IoT systems. |
| [139] | 2023 | Proof of Evolutionary Model (PoEM) | ▪ PoEM significantly enhanced consensus efficiency and security in BaaS-enabled IoT environments.<br>▪ It allowed for the inclusion of low-performance IoT devices in the consensus process, promoting wider participation.<br>▪ The protocol dynamically adapted to nodes joining and exiting, ensuring scalability and resilience.<br>▪ PoEM iteratively trained a Machine Learning (ML) model to improve consensus quality, demonstrating a novel approach to achieving consensus in dynamic IoT settings. |
| [140] | 2020 | Tree-chain | ▪ Tree-Chain is a fast and lightweight, making it suitable for the constrained environment of IoT networks.<br>▪ Tree-chain demonstrates significantly improved performance in terms of speed and resource consumption compared to traditional BCT consensus mechanisms.<br>▪ The algorithm leverages a tree-based structure to streamline the consensus process, reducing the computational overhead and energy consumption typically associated with BCT. |

Numerous benefits of smart contracts, such as increased speed, accuracy, transparency, and efficiency, have spurred the advent of innovative applications across various fields. They enhance security, diminish reliance on intermediaries, and reduce transaction costs by converting legal obligations into automated processes. Nonetheless, the adoption of smart contracts is not devoid of challenges [128]. The delegation of contract execution to computerized protocols exposes them to technical

vulnerabilities such as malware, hacking, software bugs, or communication breakdowns. The immutable and irreversible nature of BCT further amplifies the risks associated with coding errors in smart contracts [8], [129].

To ensure the widespread adoption and safe utilization of smart contracts by both consumers and providers, it is imperative to develop mechanisms for verifying and validating their correct operation. The formal validation of contract logic and its applicability remain a critical area of research, with significant contributions expected in the forthcoming years. This ongoing research is essential for overcoming the inherent vulnerabilities of smart contracts and realizing their full potential in automating and securing digital transactions and agreements [17].

### 3.7. Cryptocurrency

Built upon networks distributed across numerous platforms, cryptocurrency represents a novel category of digital assets. This digital asset class maintains its value independent of centralized authorities or the backing of financial institutions. The underpinning decentralized architecture of cryptocurrencies allows for their operation outside the purview of governmental oversight. The cryptographic techniques used to secure these networks give rise to the name "cryptocurrency". BCT plays a pivotal role in the infrastructure of many cryptocurrencies, serving as a transparent mechanism for recording transactional data [129].

Despite their innovative potential, cryptocurrencies have been subject to scrutiny due to their association with illicit activities, susceptibility to exchange rate volatility, and underlying technological vulnerabilities. However, the BCT foundational to cryptocurrencies offers several advantages, including divisibility, portability, resistance to inflation, and transparency. These attributes highlight the transformative potential of BCT and related technologies in the fields of business and finance. Consequently, it becomes imperative to navigate the legal and regulatory landscapes that will shape the future of these technologies [105].

**Table 6. IoT access control using BC.**

| Year | Paper | Contribution | Features |
|---|---|---|---|
| 2025 | [141] | MEDACCESSX utilizes BCT to ensure transparent, secure, and auditable access to medical data within IoMT networks. | ▪ It integrates a hybrid model of Attribute-based Access Control (ABAC) and Role-based Access Control (RBAC) to provide dynamic and flexible access control based on both real-time attributes and user roles.<br>▪ The framework automates data access and management using smart contracts, eliminating the need for manual intervention and ensuring efficient, fine-grained control over data sharing. |
| 2025 | [142] | AccessChain introduced a scalable and privacy-preserving access control system designed for BC-based IoT environments. | ▪ A scalable edge computing architecture that enhanced system performance.<br>▪ Privacy-preserving attribute-based encryption that ensured device privacy.<br>▪ A smart contract-based access control mechanism for reliable and secure data access. |
| 2024 | [143] | BEAC enhanced the scalability, security, and performance of access control in IoT networks. | ▪ A BCT Embedded Access Control (BEAC) designed for decentralized access control in large-scale P2P IoT systems with substantial IoT resource sharing.<br>▪ The use of BFT consensus ensures that the system can handle failures and recover access control states.<br>▪ The BEAC framework supports various access control models, making it adaptable for different IoT environments and use cases. |
| 2024 | [144] | CP-ABE e supports a more flexible access structure and large universe attributes, which is suitable for cloud-assisted EHR systems. | ▪ A Ciphertext-Policy Attribute-based Encryption (CP-ABE) combines consortium BCT and smart contract to provide secure and reliable search and outsourcing decryption.<br>▪ This model reducing the computational overhead of data users. |
| 2023 | [145] | SD-IoT enables centralized management and monitoring of the IoT network. | ▪ The article proposes a novel solution that integrates BCT and Software-Defined Networking (SDN) to create a scalable, immutable, and automated access control system for IoT networks. |
| 2023 | [146] | ABAC prevents unauthorized access to IoT devices at the network. | ▪ Attribute-based access control (ABAC) integrates with the 5G service-based architecture.<br>▪ ABAC offers a more efficient method for managing access control within the IoT landscape in the context of 5G networks |
| 2022 | [143] | ABAC-HLFBCT addressed the challenges of centralized access control mechanisms in IoT environments. | ▪ Attribute-based access control model using Hyperledger Fabric BCT (ABAC-HLFBC) utilizes smart contracts to achieve a flexible, scalable, and fine-grained access control process. |
| 2021 | [147] | A multi-agent system to provide lightweight, decentralized IoT access control security mechanisms. | ▪ BCT Managers (BCMs) provide access control and secure communication between local IoT devices, fog nodes, core fog nodes, and cloud computing. |

### 3.8. Access Control

Computers manage various sources, including memory, disk, network interface, and printer (object access). The user has access to the resources of the computer system [12]. Access control can identify unauthorized access and control individuals' access to restricted regions [8]. Controlling access to IoT devices is complex due to their constrained battery life, computing capabilities, storage, and network capacity [143]. Many studies have shown that the implementation of access control mechanisms via BCT in IoT networks can substantially improve overall network security. By leveraging BC's decentralized characteristics and

immutable ledger, we can implement access control measures more effectively and transparently, reducing the risk of unwanted access and guaranteeing that only authenticated entities can interact with IoT devices [17]. Table 6 presents some research contributions in the field of IoT access control using BCT.

## 4. BLOCKCHAIN -BASED INTERNET OF THINGS INTEGRATION

IoT is optimizing and reshaping physical procedures by transforming them into elements of the digital era. This transformation continuously generates vast volumes of data, providing unprecedented insights and knowledge. This amount of data helps to improve the quality of life through the digitalization of services in every primary sector. The implementation of IoT integrated with cloud Computing has provided outstanding effectiveness [148]. This combination has already demonstrated significant results. Likewise, BCT holds the potential to revolutionize the current IoT architecture, and the integration of both technologies can deliver substantial value [149].

The challenges inherent in IoT systems, such as resource-constrained end devices, vulnerabilities concerning privacy and confidentiality, and heterogeneity, can be mitigated through the integration of BCT [16, 150]. BCT has the potential to strengthen multiple dimensions of IoT, offering numerous potential benefits, which are highlighted below.

### 4.1. Enhanced Security

BCT enhances the security of data generated by the IoT by storing it in the form of encrypted and cryptographically validated transactions. Additionally, the integration of BC-enabled automatic software updates for IoT devices addresses potential security vulnerabilities, thereby strengthening the overall resilience of the system against breaches [151].

### 4.2. Improved Interoperability

BCT can enhance the interoperability of IoT systems by storing and modifying data generated by IoT devices in BCs. Different types of IoT datasets are transformed, mined, processed, resized, and ultimately recorded in the decentralized distributed ledger [16].

### 4.3. Autonomous Interactions

Automatic interaction of IoT devices is an excellent feature that BCT can provide. Decentralized Autonomous Corporations (DACs) are proposed for automating transactions involving large payments where traditional agencies play no role [152]. DACs are implemented by smart contracts and operate autonomously without human interference, thereby reducing costs. This functionality could also benefit IoT applications by allowing them to implement decoupled and device-agnostic applications.

### 4.4. Reliability

Since the information in BC-based systems remains distributed across the entire network and immutable over time, system members can authenticate the data and have confidence that it has not been tampered with. Additionally, BCT can provide sensor data accountability and traceability [33].

### 4.5. Trusted and Distributed Authentication

BCT provides trusted, unique, and distributed authentication of IoT devices. Through its consensus mechanism, every IoT device can be identified and authenticated, ensuring a higher level of trust. This decentralized approach eliminates the need for central authorities and offers secure, transparent, and immutable records of IoT interactions [153].

### 4.6. Secure Code Deployment

Code can be securely and safely deployed by leveraging immutable storage secured by BC. By leveraging this feature, IoT systems can use this functionality to update the device's software safely and securely during the update process [154].

### 4.7. Service Market

By enabling transactions between peers without central authorities, BCT can accelerate the development of IoT information and service systems, where microservices can be effortlessly installed and micro-payments can be made securely in a fully proofed environment [16].

### 4.8. Dependability and Traceability

BCT enhances traceability by enabling the validation and identification of IoT data anytime, anywhere [153]. All of the transactions recorded on the BCT are traceable. Wang et al. [155] developed a product traceability network based on the BCT system, which ensures the availability of product tracing services to retailers and suppliers. Moreover, the immutability feature of BCT provides the dependability of IoT data, as it is nearly impossible to alter or modify the data, since recorded information is virtually immutable.

With the continuous growth of physical devices connecting to the Internet, system vulnerabilities are increasing at an exponential rate, leading to complex security implications. In IoT systems, end devices are at a high risk of attacks, including eavesdropping, DDoS, blackholing, message fabrication, and MITM attacks [16]. As observed in botnet attacks, a group of malicious devices or nodes can collectively attack to compromise the entire IoT service framework [156]. Moreover, a central point of failure within a centralized architecture not only risks accessibility but also risks authorization and privacy [157]. Currently, security mechanisms implemented in the IoT network are centralized and comprise third-party agencies. In contrast, a BC-based IoT framework is less vulnerable to falsified validation since the transaction-issuing devices have their BCT addresses. Moreover, the consensus mechanisms implemented in public BCT systems protect against DDoS attacks by imposing a fee for every transaction [158]. Therefore, IoT security measures can be improved by implementing BCT in the system. Utilizing BCs for security policy prosecution and maintaining an openly inspectable ledger of IoT interactions, exclusive of the third-party security dependence, can be extremely advantageous to the IoT network. Various types of BC-based security improvements achieved in an IoT system are explored in the subsections below.

## 5. BLOCKCHAIN -BASED INTERNET OF THINGS APPLICATIONS

Researchers and Developers around the world are innovating ingenious ways to integrate BC-based IoT [7]. These applications focus on taking benefits from the features of BC, such as fault tolerance, immutability, cryptographic security, capability to run smart contracts, decentralized control, authentication, and data integrity. Some of the applications use patented BCs developed for their particular needs rather than using open-source BCs like Ethereum and Hyperledger. The following subsections discuss various IoT applications that have implemented BCT to enhance security.

### 5.1. Intrusion Detection System

As networks shift towards wireless applications, the increasing threat of attacks becomes a marked consideration. Various intrusion detection methods can be used to distinguish these attacks. These methods are vital for detecting unauthorized network breaches and unauthorized access to sensitive information. Consider a scenario where both a temperature sensor and a device containing sensitive data are connected to the same network. If the sensor is compromised, it may gain access to the sensitive files and potentially leak them. Naturally, users want to ensure that sensitive devices are only accessible by trusted devices. However, identifying whether a device is rogue and assessing the risk it poses to the network is neither intuitive nor straightforward, especially for end users. To provide a better user experience, it is essential to automate as much of the risk management process as possible, thereby minimizing the need for user intervention.

**Table 7. BC-based IDS.**

| Year | Paper | Contribution |
|---|---|---|
| 2025 | [159] | The proposed hybrid framework integrates Deep Learning (DL) and BCT to enhance intrusion detection and data security in IoT environments. |
| 2025 | [160] | Designing a novel, scalable, and privacy-preserving network IDS that integrates CNN, LSTM, Federated Learning (FL), BC, and explainable AI, achieving 98.2% accuracy and a low false positive rate. |
| 2024 | [161] | In The Honeypot and BC-based Intrusion Detection and Prevention (HB-IDP) model, suspicious data are forwarded for intrusion detection to the edge level; here, a honeypot is deployed to attract the attacker's patterns. |
| 2024 | [162] | The framework is known as MSecureChain and employs decentralized authentication and access control and FL-based intrusion detection in a metaverse context for KDN smart devices. |
| 2024 | [163] | The proposed work has a three-layered architecture for a distributed IDS aimed at securing data sharing between various IDS. The upper layer of the cloud service stores the required data permanently for future analysis, the fog layer is supported with BCT functionality, and the bottom layer uses multiple IDS. |
| 2024 | [133] | The proposed BC-assisted Lightweight IDS (BL-IDS) validates the authenticity of the mobile node using a Hybrid Authentication Mechanism (HAM) that combines multiple authentication aspects. |
| 2024 | [164] | A distributed federated intrusion detection method uses labeled data to identify new attack types, incorporating BCT for consensus. |
| 2023 | [57] | The proposed MetaCIDS is an innovative Cyber IDS framework designed for the metaverse based on BCT and online FL using an attention mechanism and semi-supervised learning with privacy preservation. |
| 2023 | [55] | The authors A long short-term memorys in [23] addressed the application type of healthcare monitoring, securing the Internet of Medical Things, and security of medical records using a private BC. |
| 2022 | [165] | A new approach to using BCT is proposed to enhance data processing security. Each data block is kept safe in a private cloud database. |
| 2021 | [166] | A BC-based Federated Forest SDN-enabled IDS (BFF-IDS) was developed to address the challenge of sharing sensitive data. The BFF-IDS models were hosted on the InterPlanetary File System (IPFS) to ensure BCT scalability. The model was trained and tested using the Ethereum BCT and a Mininet simulator in a local environment on the CAN-intrusion dataset. |
| 2021 | [167] | A BCT challenge-based CIDN framework that integrates BCT with a consistent challenge-based trust mechanism. The framework evaluates a node's trustworthiness by systematically analyzing the correspondence between issued challenges and the responses received. |

Thus, proposals to secure and automate home networks using IDS and Intrusion Prevention Systems (IPS) have been proposed in both researches, such as IoT-IDM and security risk management solutions [2, 168, 169]. The integration of BCT with IDS aims

to improve the accuracy, transparency, and reliability of detecting intrusions in networks [170]. Table 7 summarizes some paper contributions to BC-based IDS.

Recent prior research shows that many IDS initiatives have been developed and evaluated using public datasets or datasets provided upon request. Several published studies were reviewed, highlighting IoT security in different fields, such as the CAN bus dataset and network IDS dataset.

(1) Network Intrusion Detection System Dataset

Recently, several studies have explored the use of BCT to enhance the effectiveness of IDS within the IoT domain (as shown in the table). IDS are designed to detect unauthorized intrusions and mitigate security threats by leveraging ML models. In this context, BCT is utilized to verify the integrity of the IDS dataset and provide transparency in security operations. However, a major challenge lies in identifying suitable cybersecurity datasets for BC-based IDS implementations [14], and the creation of new, comprehensive datasets remains a complex task [171]. Several of these IDS datasets have been utilized to assess automotive IDS in IoT systems [171, 172]. Table 8 analysis of IDS datasets that have been used in IoT.

**Table 8. IDS datasets used in IoT.**

| Dataset | Number of features | Number of instances | Name of attacks | Articles that used the dataset |
|---|---|---|---|---|
| CICIoMT2024 [173] | 44 | 8,775,013 | Spoofing, MQTT, Recon, DoS, and DDoS. | [174, 175] |
| CICIoT2023 [176] | 47 | 93,373,158 | Mirai, Spoofing, Brute Force, Web-based, Recon, DoS, and DDoS. | [177, 178] |
| DDoS (CICEV2023) [179] | 7 | N/A | Wrong CS Timestamp, Wrong EV Timestamp, Wrong EV, and Correct EV ID. | [180, 181] |
| CICIoT2022 [182] | 48 | N/A | RTSP brute-force attack and flood denial-of-service attack. | [183, 184] |
| MQTT-IoT-IDS2020 [185] | 44 | 22,076,997 | MQTT brute-force attack, Sparta SSH brute-force, UDP scan, and aggressive scan. | [186, 187] |
| BoT-IoT [188] | 10 | 73,360,882 | Data Theft, Keylogging, DoS, DDoS, OS fingerprinting, and service scanning. | [189, 190] |
| CSE-CIC-IDS2018 [191] | 80 | 4,525,399 | SQL injection, Infiltration, Dos, Brute Force, and Bot. | [192, 193] |
| CICIDS2017 [13] | 79 | 2830743 | Heartbleed, Web Attack-Sql Injection, Infiltration, Web Attack – XSS, Web Attack – Brute Force, Bot, DoS Slowhttptest, DoS slowloris, SSH-Patator, FTP-Patator, DoS GoldenEye, DDoS, PortScan, and DoS Hulk. | [52, 194] |
| UNSW-NB15 [182] | 49 | 2540044 | Worms, Exploits, Generic, DoS, Backdoors, Shellcode, Analysis, Reconnaissance, and Fuzzers. | [195, 196] |
| ISCX2012 [197] | 14 | 2,545,935 | DDoS, DoS, Brute force SSH, and Infiltrating. | [198, 199] |
| NSL-KDD [112] | 42 | 148,517 | U2R, R2L, Probe, and Dos. | [200, 201] |

(2) CAN Bus dataset

A variety of open-access CAN datasets have been presented in the literature. Many of these CAN datasets have also been utilized to evaluate automotive IDS [202]. We list the existing open-access CAN datasets in Table 9.

**Table 9. Summary of CAN Bus Datasets.**

| Year | Name | Acronym | Vehicle(s) | Number Attacks | Labeled? | Real? |
|---|---|---|---|---|---|---|
| 2024 | IoV CAN bus [203] | CICIoV2024 | ECUs of a 2019 Ford | 4 | Yes | Yes |
| 2017 | CAN-intrusion [204] | OTIDS | Unknown | 4 | Yes | Yes |
| 2018 | HCRL Survival Analysis dataset [205] | HCRL SA | Chevrolet Spark, Hyundai YF Sonata, Kia Soul | 4 | Yes | Yes |
| 2019 | AEGIS Big Data Project Automotive CAN Bus [206] | AEGIS CAN | Opel Astra, Renault Clio, Testbed | 0 | N/A | Yes |
| 2020 | ML350 CAN Bus [207] | ML350 CAN | Mercedes ML350 | 2 | Yes | Yes |
| 2021 | HCRL Attack & Defense Challenge [208] | HCRL A&D | Hyundai Avante CN7 | 4 | Yes | Yes |
| 2021 | Heavy-Duty Truck CAN Bus [209] | Heavy Duty CAN | Renault T520 6X2 | 0 | N/A | Yes |
| 2023 | Can-Train-and- Test dataset | CT&T | hevrolet Impala, Chevrolet Silverado, Chevrolet Traverse, Subaru Forester. | 9 | Yes | Yes |

## 5.2. Healthcare

Currently, healthcare is witnessing significant development as a result of the development of the IoT, BC, and wearable sensor technologies, which have led to improvements in the health sector in many applications, such as patient tracking, disease prediction, infectious disease-fighting (COVID-19), electronic medical record management, remote patient monitoring, and drug traceability. Azaria et al. [210] developed a prototype named "MedRec", which provides a platform for the immediate and seamless storage of healthcare records, ensuring compatibility with other systems. Linn Azaria et al. [211] investigated the main challenges associated with using a Bitcoin-like open-source software, BC, for storing medical data. The main challenge is that

medical data requires significant storage, which complicates the scalability of the system. When a digital medical record is generated, it is authenticated with a digital signature from either the responsible doctor or the patient. The author proposed that instead of storing the entire medical record, we should only keep searchable meta-information, hash pointers, and encrypted data related to the medical records on the public BC. All actual health information would be kept separate from the BC.

### 5.3. Business Models

BCT promotes the growth of entirely new businesses and can contribute towards the shutdown of traditional incumbents. Tumasjan et al. [212] examine how BCT enables decentralized business models (BDBMs) by removing intermediaries and distributing control across networks, with applications in industries like finance, healthcare, and supply chains. Akanfe et al. [13] proposed a Sustainable Circular Business (SCB) model that integrates BCT with Circular Supply Chain Management (CSCM), enabling businesses to reduce costs, improve ecological sustainability, and optimize performance through smart contracts, transparency, and efficient resource management. Upadhyay et al. [213] presented a framework for developing BCT business models, emphasizing the importance of aligning key components like value propositions, resources, and partnerships to leverage BC's decentralized features. It provides organizations with tools to assess and optimize their models, helping them capture value and drive innovation using BCT. Schneider et al. [214] designed a theoretical framework to analyze the implications of BCT on value creation. The framework offers that BCT operates as an agent, a capability, and a resource for its users. As a result, it donates to the emergence, enablement, and efficiency progress across various business models and ecosystems.

### 5.4. Smart Home

SHIB [215] is a smart house that employs BCT with IoT to address troubles such as secure connection supervision, scalability, and data confidentiality. The architect of Access Control Code (ACC) has exclusive authority to add new rules, modify existing ones, or eliminate privacy constraints on the BC. To employ this design, a responsible owner must have engaged in a smart contract with the appropriate parties. Smart contracts may limit access requests if there is network misconduct, which improves the privacy and security of home data. This approach is unique compared to other existing models because it includes a Judge Contract (JC) that has the authority to make decisions and impose fines in cases of misconduct [3]. An authentication technique that guarantees privacy is presented to explain the process of sharing and collecting data in smart home applications [216]. The proposed approach integrates three fundamental principles: smart contracts, intellectual edges, and attribute-based access control, to produce a secure and resilient architecture. Data is securely and confidentially moved to the cloud using a differential privacy approach. This approach alleviates the computational load on systems, thereby enhancing their adaptability. The proposed system architecture consists of clients, IoT devices, multi-edge computers, and the cloud. Attribute-based access control employs two sorts of conventions: authorization contracts and access contracts. The authors thoroughly account for the transaction process, including four separate stages: linked transaction, status delivery, request administration, and initialization. The variation security enhancement approach consists of a fundamental method, a hidden strategy, a set of information, and implementation. The suggested method outperforms the present technique by offering enhanced security, privacy, resilience against assaults, precise access control, and reduced computational expenses.

### 5.5. Smart Cities

A smart city presents a higher quality of life to residents by maximizing resource utilization and promoting transparency in governance. These cities are built by integrating and connecting different systems and infrastructures utilizing communication technologies, which work collectively to generate intelligent information.

Sabrina [217] suggested an approach for managing access to resources in comprehensive IoT systems, such as those seen in smart cities. Public smart contracts and the BCT are utilized for external access control, whilst regional off-chain storage is used for internal access control. In another study, Makhdoom et al. [218] presented a BCT architecture for smart city security. Hakak et al. [219] presented "PrivySharing," a BC-Based security architecture for secure IoT data exchange in smart cities. BCT is separated into channels with specialized data from a limited number of authorized organizations to ensure data privacy. Additionally, data in these channels is collected and encrypted privately to provide isolation and security.

### 5.6. Supply Chain Management

The primary application of BCT in supply chain management is to trace and keep track of the products and maintain visibility throughout the process. Additionally, BCT enhances the security of information sharing among all the commodities involved in the supply chain. Sharing and tracing information about the product not only prevents counterfeiting of products but also provides transparent information about the product. Ethereum BCT with BigChainDB, PoC, off-chain storage, and double chains are some of the solutions proposed by researchers. To enhance monitoring and real-time tracking, Ethereum and Hyperledger Sawtooth

combined with IoT and RFID, have been used to ensure the unique identification of items. Additionally, some other researchers discussed Hyperledger Fabric BCT as it has better performance [7].

### 5.7. Education

Privacy challenges could hamper the acceptance of BCT in education, as some educational institutions may have a low degree of openness to their learning resources [220]. New research illustrates the potential of BCT in education [221]. BC-based applications are fast emerging in numerous domains of education, including competency and learning outcome management, copyright management, student assessments and examination systems, and professional capability assessment [222]. A common approach is used by EduCTX, a platform for recording credentials [40], as well as other educational data management systems to effectively and securely store students' academic records and credentials [41]. The use of BCT in education enables transparent data management and verification. Gottlieb et al. [223] explored the potential of BCT applications in higher education institutions (HEIs), focusing on credential verification, record-sharing, and reputation management. It highlights the advantages of BC, such as increased security, transparency, and efficiency, in addressing HEI administration challenges like record-keeping and certificate validation while providing a detailed assessment of both application-level and protocol-level implementations. The previously discussed BC-based IoT applications are summarized in Table 10.

**Table 10. BC-based IoT applications.**

| Application | Reference | Contribution |
|---|---|---|
| Healthcare | [224] | ▪ An optimized Healthcare Framework Based on BC, Delegated by Mixed Multi-Agent Reinforcement Learning. |
| | [225] | ▪ Designed a framework that combines BCT with IoT devices to address the essential challenges of data privacy and security in healthcare. |
| | [210] | ▪ A prototype named MedRec was introduced that uses BCT to store electronic health data, particularly for medical research purposes. |
| | [211] | ▪ BCT is introduced as a decentralized and secure solution for managing electronic health records (EHRs) and supporting health-related IT and research activities. |
| Business models | [13] | ▪ The conflicts between BCT immutability and privacy regulations are presented in this paper, and solutions such as privacy-preserving techniques are proposed. |
| | [213] | ▪ Empirical data were studied to classify and evaluate BC-based business models across industries, focusing on their operational mechanisms, benefits, and challenges. |
| | [214] | ▪ Framework to analyze BCT implications on value creation. |
| | [226] | ▪ Bitcoin-based business process management system is proposed for seamless verification and execution monitoring of choreographies while preserving the independence and anonymity of the participants. |
| Smart home | [227] | ▪ BCT has been used to secure data exchange and improve privacy, security, and authentication in smart home IoT networks. |
| | [216] | ▪ A BC-based privacy-preserving mechanism that secures personal data in smart homes is proposed. |
| | [228] | ▪ A framework is proposed that uses BCT to provide secure communications, data integrity, and privacy for IoT devices in smart homes. |
| Smart cities | [217] | ▪ This study presents a method for managing access to resources in dense IoT systems, particularly in smart cities. |
| | [218] | ▪ BCT architecture for smart city security introduced. |
| | [219] | ▪ The PrivySharing architecture is introduced as a BC-based security architecture for securely exchanging IoT data in smart cities. |
| Supply chain management | [229] | ▪ The implications of BCT on supply chain decision-making are investigated.<br>▪ An Italian airport has deployed a BC-based collaborative decision-making platform that fosters collaboration between air traffic controllers and the aviation industry. |
| | [230] | ▪ A BC-based product information traceability framework is proposed to achieve effective label verification in cross-border e-commerce supply chain. |
| | [231] | ▪ The integration of BCT and supply chains has been proposed to achieve sustainability. |
| Education | [232] | ▪ This study demonstrates that BC-based decentralized applications can provide a secure, tamper-resistant, and efficient way to share student credentials. |
| | [223] | ▪ Various applications of BCT in higher education are identified. Also addressing challenges like scalability and adoption barriers. |
| | [233] | ▪ The student work evaluation model (CLSW) is proposed to enhance the educational process. |
| | [220] | ▪ BCT has been used to manage online learning. |

## 6. CHALLENGES, FUTURE RESEARCH DIRECTIONS, AND OPEN ISSUES

This section provides an overview of the challenges, future research directions, and outstanding issues in integrating BCT with the IoT. The challenges are classified into three categories: challenges related to the IoT, BC, and the integration of BCT with the IoT.

### 6.1. Challenges Related to Internet of Things

Many challenges must be addressed to better realize the IoT vision. To ensure the adoption and widespread use of IoT, these challenges must be addressed effectively [33, 234]. This review introduced some of the IoT challenges, which are detailed in Table 11. These challenges reflect both the technical and operational complexities of implementing IoT systems across diverse sectors.

**Table 11. IoT Security Challenges.**

| Challenge | Description & References |
|---|---|
| Architecture | Since IoT encompasses a wide range of smart sensors and devices utilizing various technologies, a single reference architecture cannot serve as a blueprint for all application requirements [20, 33, 40, 47, 48, 235]. |
| Transmission Control Protocol (TCP) | The TCP is generally unsuitable for managing end-to-end transmission control in IoT [33, 236]. |
| Operating System (OS) | The optimal OS for IoT has not been born yet [32, 33, 237]. |
| Heterogeneity | The diversity in IoT device operating conditions, functionalities, and resolutions creates heterogeneity, which makes seamless integration difficult [238, 239]. |
| Security and Privacy | IoT devices gather private information, which makes data theft, unauthorized access, and privacy violations more likely. Strong security must be ensured [14, 17, 33, 51]. |
| Interoperability | The wide range of IoT devices employs different communication standards and protocols, resulting in interoperability and inefficient integration [33, 73, 167, 238, 240]. |
| Scalability | The increasing number of IoT devices presents significant challenges for network scalability and management. These challenges complicate the handling of large data volumes and numerous devices [33, 127, 134, 238]. |
| Data Management | IoT generates large volumes of data, making storage, processing, and analysis increasingly difficult, especially in real-time scenarios [33, 237]. |
| Energy Efficiency | Many IoT devices rely on battery power, so energy management and efficiency are critical to extending device lifespans and reducing maintenance costs [33, 241]. |
| Latency and Real-time Processing | IoT applications, especially in critical sectors like healthcare and automotive, require low latency and real-time data processing for responsiveness [242, 243]. |
| Cost of Deployment | Implementing IoT solutions, including sensors, connectivity, and infrastructure, can involve significant upfront and ongoing operational costs [33]. |
| Device Management | It's difficult to maintain system health, manage a large number of IoT devices in different environments, and make sure firmware updates are made [33, 241, 244]. |
| Bandwidth Constraints | IoT devices frequently operate in bandwidth-constrained environments, necessitating effective optimization and data transmission strategies [33, 241]. |
| Network Reliability | Even in places with spotty or inconsistent network conditions, IoT networks need to be able to maintain consistent and dependable connections [33]. |
| Lack of Standards | It is challenging to achieve consistent performance, security, and communication when there are no universal IoT standards, which causes fragmentation [33]. |
| Analytics and Insights | To extract valuable insights from massive IoT data sets, we need large-scale ML, Artificial Intelligence (AI), and advanced analytics tools. These processes can be resource-intensive [33]. |
| Legal and Regulatory Compliance | IoT deployments have to abide by a number of local, national, and international laws pertaining to privacy, data security, and safety requirements [51]. |
| Limited Processing Power | Many IoT devices have limited computing power, making it difficult to implement strong security measures or process data locally [33, 241]. |
| User Adoption and Understanding | Many potential users lack awareness or understanding of IoT technology and its benefits, which can hinder adoption in both consumer and industrial settings [244]. |

### 6.2. Challenges Related to Blockchain

While BCT offers numerous advantages, including transparency and security, these challenges highlight the need for ongoing research and development to improve scalability, energy efficiency, and regulatory compliance [245, 246]. To ensure successful adoption, we must address several challenges associated with BCT implementation. In addition to issues like scalability, interoperability, privacy, and confidentiality. Some of the most common challenges faced in the BCT are explored in the subsections below Table 12.

**Table 12. BCT Challenges.**

| Challenge | Description & References |
|---|---|
| Security Issues | 51% Attacks: A 51% attack transpires when malevolent entities dominate over fifty percent of the network's mining capacity, enabling them to modify the BC, manipulate transactions, or engage in double-spending of currencies [17, 245].<br>Smart Contract Vulnerabilities: Although BCT is secure, improperly programmed smart contracts, which automate processes on the BC, might expose weaknesses that may be exploited [8, 246]. |
| Scalability | Transaction Throughput: Public BC, such as Bitcoin and Ethereum, have a finite capacity for transactions processed per second. For large-scale applications such as IoT, where millions of transactions transpire concurrently[245].<br>Data Growth: Every transaction is recorded on the BC, which results in a rapidly growing ledger. This growing size requires nodes to store increasing amounts of data, which can be problematic over time [74]. |
| High Energy Consumption | Consensus Mechanisms: Certain consensus protocols used in the BCT network consume more energy, and this raises concerns about the environmental impact and sustainability of such networks [14, 17, 246]. |
| Latency | Validation Time: in public BC, it can take several minutes to validate a transaction due to the time-consuming consensus process [12, 245]. |

| | |
|---|---|
| Interoperability | Various BCT platforms frequently function in isolation, each with distinct standards and protocols. This presents difficulties in integrating multiple BCT or employing BCT across diverse industries or platforms [246]. |
| Regulatory and Legal | Lack of Regulation: the legal status of BCT transactions, including cryptocurrency transactions, differs significantly across nations. This ambiguity poses risks for enterprises seeking to implement BCT while uncertain about the forthcoming legal framework [245].<br>Compliance: BCT implementation must comply with specific legal and regulatory requirements. The decentralized and immutable characteristics of BCT may conflict with specific data protection and privacy regulations, potentially resulting in compliance challenges [14, 246]. |
| Cost of Implementation | Establishing and sustaining BCT infrastructure can be expensive, particularly for enterprises necessitating extensive implementation. The requisite computational power, coupled with substantial energy consumption, renders BCT costly for enterprises [246]. |
| Security Issues | While BCT is implemented to enhance the security of end applications, it remains vulnerable to potential attacks. Vulnerabilities in smart contracts, attacks on consensus mechanisms like proof-of-work, and the hacking of cryptocurrency exchanges are specific security concerns affecting the BCT network [14, 17]. |
| User Experience | The user experience of BC-based applications can be intricate and daunting for non-technical individuals; thus, it is crucial to enhance accessibility and user interface to improve real-time application experiences [14]. |
| Upgrade and Fork Management | Updating and managing network forks in BCT models can be intricate and demanding. Coordinating network upgrades while achieving consensus among participants is challenging [14]. |
| Lack of Awareness | Due to the nascent nature of BCT, there exists a deficiency in comprehension and awareness regarding its potential advantages and constraints. It is essential to instruct stakeholders on the effective implementation of BCT for IoT security [14]. |

### 6.3. Challenges Integration of Blockchain with Internet of Things

Although integration of IoT and BCT brings many improvements (as shown in Section IV), it also introduces notable security challenges. The following subsections examine these key challenges.

(1) Security

Numerous studies have identified BCT as a critical component for the much-needed improvement in IoT security. However, a significant obstacle to BC-based IoT integration is the reliability of the data produced by IoT devices. BCT provides transaction validation and data immutability, yet the chain retains incorrect data once introduced.

Bhattacharjya et al. [247] have identified additional threats such as eavesdropping, MITM, and service rejection. Due to their susceptibility to hacking and attacks, potential security flaws or breaches prevent the gadgets from functioning properly. IoT device communication may suffer significantly from the combination of BCT with IoT. Currently, IoT application protocols like CoAP (Constrained Application Protocol) use safety protocols like TLS (Transport Layer Security) or DTLS (Datagram Transport Layer Security) to facilitate communication and MQTT (Message Queuing Telemetry Transport). These protocols are complicated and weighty, though [16, 248].

(2) Consensus

The resource constraints imposed by IoT devices make them inadequate for directly implementing consensus techniques like PoW. As previously stated, many proposals for consensus procedures exist, although they frequently remain underdeveloped and inadequately tested. Although there are various plans to include complete BCT nodes inside IoT devices, mining continues to pose a significant difficulty within the IoT domain [16].

(3) Storage capability and scalability

The main challenge in integrating BC-based IoT is BC's limited storage capability and scalability, which are problematic for IoT's large data volumes. Addressing these challenges is critical for successful integration. Currently, most of the data gathered from the devices is stored, while a small portion is used to inform actions and extract knowledge. Theoretically, various techniques for compressing, normalizing, and filtering data have been proposed. Data compression can enhance the storage, transmission, and processing of large volumes of IoT-generated data [16].

(4) Smart contracts

IoT can benefit from smart contracts, and the IoT framework can implement them in a variety of ways. Smart contracts can ensure a dependable and safe processing engine. Although certain challenges exist, it's important to consider them beforehand. At times, the instability of the IoT structure could compromise the validation and verification of these contracts. Retrieving data from different sources could further overload the contracts. Despite the decentralized and distributive nature of smart contracts, they do not share the resources to perform extensive processing, as the contract code executes simultaneously in every node. To meet the needs of IoT, smart contracts should include group mechanisms and filtering features [78, 155].

(5) Data privacy and anonymity

Many IoT applications handle private data, making privacy and confidentiality critical at all stages, which increases the complexity of BCT itself, as they begin with the data assortment stage and extend to the communication and application stages. The integration of cryptographic software into devices presents significant security challenges. Additionally, we must consider the limitations of computational resources and economic viability constraints. Due to inherent limitations, IoT devices frequently

depend on encryption standards such as Internet Protocol Security (IPSec), Secure Socket Layer (SSL), and TLS to ensure secure communication. Additionally, the integration of BCT can enhance trust within IoT systems [215, 249].

(6) Legislative issues

BCT, especially in the context of cryptocurrencies, has raised many questions about authenticity. National data privacy laws also impact the IoT, as seen with data protection directives. As new technologies emerge, many existing laws become outdated and require updates. Creating new standards and rules can sometimes weaken device security, but it can also help build more reliable and secure IoT networks. However, differences in information handling and security laws across countries pose a significant challenge to managing IoT. This challenge becomes even greater when BCT is involved [97].

### 6.4. Future Directions and Open Issues

This section explores the open issues and potential research directions that may facilitate the exploration of multiple aspects of BC-based IoT integration. Despite the number of survey studies in the literature, some research gaps need more attention. For instance, the Authors in [12] provided a thorough review of BC-IoT integration in healthcare applications. It identifies numerous challenges associated with implementing BCT in IoT healthcare systems, such as privacy, security, interoperability, and scalability, and proposes potential solutions for these issues. Besides, the study does not address in detail how different BCT types and configurations can effectively handle large-scale data integration in IoT systems. Fazel et al. [250] discussed the potential of integrating IoT with advanced technologies such as ML and BCT in various sectors, such as healthcare, transportation, and supply chain management. This study identified open research issues and suggested future directions for advancing the integration of IoT with ML and BC, providing a roadmap for further investigation. Besides, the study does not provide comprehensive strategies to mitigate these challenges in a practical context. Gugueoth et al. [14] identified and categorized a wide range of IoT security threats, such as impersonation, eavesdropping, and denial-of-service attacks, and discussed how BCT can help mitigate these threats. The research investigated various consensus algorithms, including PoW, PoS, and PBFT, and evaluated their suitability for IoT systems. Besides, the study does not provide comprehensive strategies to mitigate these challenges in a practical context. The authors in [251] discussed various consensus algorithms, cryptographic techniques, and privacy-preserving mechanisms, offering insights into how these solutions can improve the security and privacy of healthcare data. The study does not delve deeply into the resource limitations of BC, such as computational power and energy consumption, which are critical considerations for deploying BCT in real-world healthcare applications. As observed, the studies have mainly focused on network attacks and architectural details, and little attention has been paid to the possible solutions and the need for BCT integration with IoT to enhance security. This limitation is addressed in the current review, and solutions for their limitations are discussed. In addition to these research gaps, other issues need to be addressed. However, it does not propose detailed solutions for overcoming these challenges. The following issues and opportunities can improve the security capabilities of BC-IoT.

(1) Machine Learning Solution

ML and BCT can improve platforms and hardware by overcoming specific challenges. The integration of ML, BC, and the IoT in healthcare has the potential to enhance patient outcomes and reduce costs considerably. ML and the IoT can facilitate real-time monitoring of chronic diseases, enhancing communication between patients and healthcare providers [252]. The implementation of Electronic Health Records (EHR), the Internet of Medical Things (IoMT), and BCT can improve data integrity and security, facilitating the sharing of medical data and clinical information [253]. The integration of IoT and big data in healthcare may facilitate the development of specific preventative health coaches able to analyze health data and help clients enhance their lifestyles [254]. The integration of IoT and BCT offers potential in supply chain management by improving transparency, reliability, and operational efficiency. These technologies are essential for enhancing transparency throughout the value chain, cultivating trust among business entities, and reducing risks within the context of the industry.

Moreover, BCT offers transformative capabilities in resolving supply chain and logistics issues, especially in guaranteeing the provenance and traceability of essential products. The importance of ML, BC, and the IoT in cybersecurity has been demonstrated by numerous research. These technologies are employed to secure connected and autonomous vehicles, safeguard industrial IoT systems, mitigate security vulnerabilities, and manage security and privacy concerns in IoT. The emphasis is on employing ML and BCT for intrusion detection and data protection, utilizing machine and DL to safeguard industrial IoT systems, and suggesting integration of BC, AI, and ML to reduce vulnerabilities [250].

As an example, Manavalan [255] emphasized the importance of integrating AI and ML with IoT to enable intelligent decision-making and the replication of behavioral patterns. The incorporation of BCT can enhance IoT security, as highlighted by Panarello et al. [75], due to its immutable characteristics and data encryption functionalities. Bacciu et al. [256] underscore the crucial function of ML in enabling IoT applications to adjust to changing conditions. Zikria et al. [257] explored the complexities of merging DL with IoT to improve network efficiency, highlighting the associated obstacles and potential. In summary, the integration of IoT and BCT in supply chain management offers potential improvements in transparency, trustworthiness, and

operational efficiency while also significantly improving cybersecurity through the utilization of ML, BC, and IoT in various security applications.

(2) Blockchain-based SDN for Internet of Things Integration

Although many research studies have developed that integrate BCT with SDN, certain challenges arise when implemented in practical IoT applications. The absence of a comprehensive cryptographic and encryption technology poses a significant challenge that affects the privacy and confidentiality of data exchanged between two entities [145]. Moreover, the challenges of addressing attacks such as MITM and DoS in B-IoT within the SDN are still important. To address this issue as an illustration, Rahman et al. [258] outline a stratified hierarchical structure for a BC-SDN-IoT framework. Rathore et al. [259] proposed a decentralized security architecture based on SDN coupled with BCT for IoT networks in the smart city. The architectures take less time to mitigate attacks in the IoT ecosystem.

(3) Computation Paradigms

One challenge relating to the convergence of the B-IoT technologies is the optimization of resource utilization in decentralized systems. A potential formula for resolving this issue is Resource Efficiency = (Energy Consumption * Computation Time) / Accuracy. This formula illustrates the trade-off between energy consumption, computing time, and Accuracy in data processing by a system. The objective is to create systems that are accurate and resource-efficient for data processing in decentralized environments [250]. To exemplify the approach taken to resolve this issue, Zhou et al. [260] proposed a collaborative approach to maintaining a comprehensive BCT in wireless IoT networks. Rahman et al. [258] developed a stratified hierarchical framework for BC-SDN-IoT integration. Munsing et al. [261] developed a peer-to-peer energy market framework utilizing BCs and smart contracts for the decentralized optimization of energy resources within microgrid networks. These investigations collectively highlight BCT's potential to reduce limitations on resources and enhance efficiency in B-IoT ecosystems.

(4) Blockchain Technology for Intrusion Detection System

Recently, several studies have explored the use of BCT to enhance the effectiveness of IDS within the IoT domain. IDS are designed to detect unauthorized intrusions and mitigate security threats by leveraging ML models. In this context, BCT is utilized to verify the integrity of IDS data and provide transparency in security operations. However, a major challenge lies in identifying suitable cybersecurity datasets for BC-based IDS implementations [14], and the creation of new, comprehensive datasets remains a complex task [171]. As an example, the authors in [262] emphasized the potential of BC-enhanced CNNs as a robust and secure solution for intrusion detection in CPS, ensuring the integrity and protection of critical infrastructure. Moreover, Table 7 summarizes some article contributions to BC-based IDS.

(5) Developing effective consensus protocols

The main consensus protocols utilized are PoW, PoS, and PBFT, as illustrated in the table. Nevertheless, these procedures fail to consider the constraints of storage space and processing power, which can negatively affect their efficacy. Consequently, it is imperative to evaluate elements such as processing speed, computational demands, and reliability while formulating a suitable consensus protocol. Future research may concentrate on creating hybrid consensus protocol algorithms that combine the advantages of multiple existing protocols to address these limitations and improve performance [133]. The authors in [263] proposed hybrid consensus algorithms, highlighting their advantages in forecasting cyber-attacks, anomaly detection, and feature extraction.

(6) Securing access to Internet of Things devices

BCT enhances dynamic access control by providing high automation and improved security, thereby minimizing the risk of access control attacks. Future research should focus on developing and standardizing techniques for integrating on-chain access control with off-chain storage. Additionally, emphasis should be placed on mitigating known access control vulnerabilities within BCT systems to enhance security and reliability further [17]. To address this issue as an illustration, [144] proposed a privacy-preserving access control with a policy-hiding scheme based on attribute-based cryptography and a consortium BC. Table 6 presents some research contributions in the field of IoT access control using BCT.

(7) 5G-enabled Blockchain-based Internet of Things networks

5G is an emerging technology poised to revolutionize existing IoT applications. The growing prominence of 5G networks relates to an increase in privacy leakage risks. Developing a robust security strategy for 5G networks is definitely tough due to their novelty, volatility, and susceptibility [146]. Promising techniques, like privacy-aware DL, reinforcement learning, and game theory, can enhance security in 5G-based B-IoT networks [14]. Djenouri et al. [264] created a comprehensive architecture for addressing the distributed knowledge graph matching issue in 5G IoT networks. The system correctly identified the shared concepts and relationships from the collection of knowledge graphs by utilizing both BCT management and AI.

(8) Secure Blockchain Technology ledgers at Fog computing

The deployment of distributed ledgers in fog computing is the most reliable and cost-efficient way to reduce latency challenges in B-IoT networks [240]. Nonetheless, maintaining the confidentiality of BCT ledgers takes a lot of work. Securing ledgers in fog

computing applications requires the evaluation of various criteria, including the selection of trusted fog nodes and the assurance of ledger secrecy, among others [14]. Therefore, carrying out research in this area is a significant challenge, and the creation of a secure, robust, dependable, and resilient mechanism for the security of BC-based fog computing applications presents a promising research opportunity. As an example, Liu et al. [249] proposed a distributed access control system based on BCT to secure IoT data based on fog computing and the concept of the alliance chain.

(9) Blockchain Technology for commercial applications

Nowadays, International trade is often seen as chaotic and inefficient, hindering commerce. Foreign trade is frequently affected by dishonesty, counterfeiting, and fraud. Adding cryptocurrency using BCT will enable us to address many of these issues. Combining payment methods, paperwork, and regulations into a single digital international system can address most fraud and inefficiency. This change will lead to increased trade and better international relations. BCT continues to develop and grow with greater advancements, not only in cryptocurrency but also in several commercial applications, including smart contracts, automated tracking, and rule enforcement. The effects of BCT will impact businesses and society [251]. The author in [265] proposed a traceability system for food products in international commerce based on BCT networks and RFID tags. This research [266] probed whether and how BCT could enhance global governance, with an illustration for climate governance. This article [267] analyzed the impacts of BCT on international business and the resulting challenges and implications for global governance.

## 7. CONCLUSION

This paper presented a comprehensive and structured review of the role of BCT in enhancing the security, efficiency, and reliability of IoT environments. Beginning with an overview of IoT, its diverse applications, components, and architectures, the survey highlighted the wide range of threats and vulnerabilities that IoT environments face, including physical, software, network, application-level, and authorization attacks. The paper then examined the core principles, types, and characteristics of BC. Moreover, this paper provides a comprehensive comparative analysis of various BCT platforms, highlighting the key properties of both private and public DLT platforms. It also includes both quantitative and qualitative evaluations of these platforms to help researchers select the most suitable platform and understand key mechanisms, such as smart contracts, consensus protocols, cryptocurrencies, and access control models.

The integration of BC-based IoT was further explored across multiple domains, including IDS, healthcare, business models, smart homes, smart cities, supply chain management, and education. These examples demonstrated that BCT not only strengthens trust and accountability but also enables more autonomous, interoperable, and resilient IoT infrastructures. Although there are promising prospects, this survey emphasizes that substantial challenges remain. Challenges inherent to both the IoT and BC, including scalability, resource efficiency, and performance, continue to impede seamless deployment. Additionally, their integration introduces further complexities related to privacy, consensus mechanisms, regulatory compliance, and secure access in dynamic environments.

Additionally, this paper identifies several future research directions with substantial potential to advance the field. Famous areas of focus include the development of lightweight consensus protocols tailored for IoT environments, the integration of ML and DL techniques to enhance the performance and accuracy of BC-based IDS, and the adoption of SDN in conjunction with edge and fog computing paradigms to improve scalability and reduce latency. Furthermore, the convergence of BCT with emerging communication technologies, particularly 5G and beyond, offers promising prospects for enabling real-time, large-scale, and secure IoT deployments.

As future work, further research is necessary to design more efficient and scalable BC-based IoT architectures, including the study of adaptive consensus mechanisms, the integration of AI for automated security monitoring, and the investigation of interoperability standards for IoT networks. Moreover, the development of IDS with BCT expresses a promising direction. Additionally, longitudinal studies and real-world deployments are critical for validating the effectiveness of BCT solutions across various application domains.

### Competing Interests

The authors declare that they have no conflict of interest.

## References

[1] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, and A. Srinivasulu, "State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions.," *Sustainability* vol. 13, no. 16, p. 9463, 2021.

[2] V. Dedeoglu, R. Jurdak, G. D. Putra, A. Dorri, and S. S. Kanhere, "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, pp. 190-199.

[3] N. T. Y. Huan and Z. A. J. I. A. Zukarnain, "A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications," 2024.

[4] P. Sun, S. Shen, Y. Wan, Z. Wu, Z. Fang, and X.-z. J. I. I. o. T. J. Gao, "A survey of iot privacy security: Architecture, technology, challenges, and trends," 2024.

[5] S. Haber and W. S. Stornetta, *How to time-stamp a digital document*. Springer, 1991.

[6] N. S. Bitcoin, "Bitcoin: A peer-to-peer electronic cash system," ed, 2008.

[7] S. Mathur, A. Kalla, G. Gür, M. K. Bohra, and M. J. C. N. Liyanage, "A survey on role of blockchain for IoT: Applications and technical aspects," vol. 227, p. 109726, 2023.

[8] V. Maurya *et al.*, "Blockchain-driven security for IoT networks: State-of-the-art, challenges and future directions," vol. 18, no. 1, pp. 1-35, 2025.

[9] N. Sharma and P. J. C. C. Dhiman, "A survey on IoT security: challenges and their solutions using machine learning and blockchain technology," vol. 28, no. 5, pp. 1-40, 2025.

[10] M. Gholami, A. Ghaffari, N. Derakhshanfard, N. iBRAHIMOĞLU, A. A. P. J. C. Kazem, Materials, and Continua, "Blockchain Integration in IoT: Applications, Opportunities, and Challenges," vol. 83, no. 2, 2025.

[11] Y. Aounzou, A. Boulaalam, F. J. I. J. o. S. S. Kalloubi, and I. Systems, "Convergence of blockchain, IoT, and machine learning: exploring opportunities and challenges–a systematic review," vol. 18, no. 1, 2025.

[12] W. A. Al-Nbhany, A. T. Zahary, and A. A. Al-Shargabi, "Blockchain-IoT Healthcare Applications and Trends: A Review," *IEEE Access*, 2024.

[13] O. Akanfe, D. Lawong, and H. R. J. I. J. o. I. M. Rao, "Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities," vol. 76, p. 102753, 2024.

[14] V. Gugueoth, S. Safavat, S. Shetty, and D. J. C. S. R. Rawat, "A review of IoT security and privacy using decentralized blockchain techniques," vol. 50, p. 100585, 2023.

[15] H. Guo, X. J. B. r. Yu, and applications, "A survey on blockchain technology and its security," vol. 3, no. 2, p. 100067, 2022.

[16] S. Saxena, B. Bhushan, M. A. J. J. o. N. Ahad, and C. Applications, "Blockchain based solutions to secure IoT: Background, integration trends and a way forward," vol. 181, p. 103050, 2021.

[17] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A survey of IoT and blockchain integration: Security perspective," *IEEE Access*, vol. 9, pp. 156114-156150, 2021.

[18] R. Thakore, R. Vaghashiya, C. Patel, and N. J. P. c. s. Doshi, "Blockchain-based IoT: A survey," vol. 155, pp. 704-709, 2019.

[19] H.-N. Dai, Z. Zheng, and Y. J. I. i. o. t. j. Zhang, "Blockchain for Internet of Things: A survey," vol. 6, no. 5, pp. 8076-8094, 2019.

[20] M. Burhan, R. A. Rehman, B. Khan, and B.-S. J. s. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," vol. 18, no. 9, p. 2796, 2018.

[21] R. Kebache *et al.*, "Reducing the Encrypted Data Size: Healthcare with IoT-Cloud Computing Applications," vol. 48, no. 4, 2024.

[22] Y. Ghoul, O. J. M. T. Naifar, and Applications, "IoT based applications for healthcare and home automation," vol. 83, no. 10, pp. 29945-29967, 2024.

[23] V. Sutar, K. J. G. I. J. o. E. Kulhalli, and Technology, "An Effective Stray Animal Detection and Crash Prevention System using Deep Learning and Internet of Things," vol. 10, no. 1, 2024.

[24] Z. Bi *et al.*, "Real-time force monitoring of smart grippers for Internet of Things (IoT) applications," vol. 11, pp. 19-28, 2018.

[25] K. S. Sudha, N. J. C. Jeyanthi, and I. Technologies, "A review on privacy requirements and application layer security in internet of things (IoT)," vol. 21, no. 3, pp. 50-72, 2021.

[26] N. Koshizuka and K. J. I. P. C. Sakamura, "Ubiquitous ID: standards for ubiquitous computing and the internet of things," vol. 9, no. 4, pp. 98-101, 2010.

[27] G. Casella, B. Bigliardi, and E. J. P. C. S. Bottani, "The evolution of RFID technology in the logistics field: a review," vol. 200, pp. 1582-1592, 2022.

[28] K. S. Mohamed, *Bluetooth 5.0 Modem Design for IoT Devices*. Springer, 2022.

[29] M. L. Hamzah *et al.*, "Implementation of the internet of things on smart posters using near field communication technology in the tourism sector," vol. 3, no. 3, pp. 194-202, 2022.

[30] M. J. Alam, M. R. Hossain, S. Azad, and R. J. T. o. E. T. T. Chugh, "An overview of LTE/LTE-A heterogeneous networks for 5G and beyond," vol. 34, no. 8, p. e4806, 2023.

[31] E. Mozaffariahrar, F. Theoleyre, and M. J. F. I. Menth, "A survey of Wi-Fi 6: Technologies, advances, and challenges," vol. 14, no. 10, p. 293, 2022.

[32] N. Al-Taleb and N. Min-Allah, "A study on internet of things operating systems," in *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, 2019, pp. 1-7: IEEE.

[33] E. A. Shammar and A. T. J. L. H. T. Zahary, "The Internet of Things (IoT): a survey of techniques, operating systems, and trends," vol. 38, no. 1, pp. 5-66, 2020.

[34] S. F. Barrett, *Arduino microcontroller processing for everyone!* Springer Nature, 2022.

[35] M. Maksimović, V. Vujović, N. Davidović, V. Milošević, and B. J. d. i. Perišić, "Raspberry Pi as Internet of things hardware: performances and constraints," vol. 3, no. 8, pp. 1-6, 2014.

[36] M. De Sousa, *Internet of Things with Intel Galileo*. Packt Publishing Ltd, 2015.

[37] M. Gigli, S. J. D. o. M. Koo, and U. o. S. D. Computer Science, USA, "Internet of things: services and applications categorization," 2011.

[38] S. Dhiviya, S. Malathy, D. R. J. J. o. c. Kumar, and t. nanoscience, "Internet of things (IoT) elements, trends and applications," vol. 15, no. 5, pp. 1639-1643, 2018.

[39] P. K. Sadhu, V. P. Yanambaka, and A. J. S. Abdelgawad, "Internet of things: Security and solutions survey," vol. 22, no. 19, p. 7433, 2022.

[40] M. G. d. Santos, D. Ameyed, F. Petrillo, F. Jaafar, and M. J. a. p. a. Cheriet, "Internet of Things architectures: A comparative study," 2020.

[41] B. Ali and A. I. J. s. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," vol. 18, no. 3, p. 817, 2018.

[42] D. U. J. T. J. o. E. ugli Jurayev and Technology, "Security in the Internet of Things: A Review," vol. 11, pp. 15-17, 2022.

[43] O. Said and M. J. I. J. o. C. N. Masud, "Towards internet of things: Survey and future vision," vol. 5, no. 1, pp. 1-17, 2013.

[44] D. J. I. J. C. A. R. Darwish, "Improved layered architecture for Internet of Things," vol. 4, no. 4, pp. 214-223, 2015.

[45] M. A. Pisching, M. A. Pessoa, F. Junqueira, D. J. dos Santos Filho, P. E. J. C. Miyagi, and I. Engineering, "An architecture based on RAMI 4.0 to discover equipment to process operations required by products," vol. 125, pp. 574-591, 2018.

[46] T. Rajmohan, P. H. Nguyen, and N. J. C. Ferry, "A decade of research on patterns and architectures for IoT security," vol. 5, no. 1, p. 2, 2022.

[47] S. A. Ansar, S. Arya, S. Aggrawal, S. Saxena, A. Kushwaha, and P. C. Pathak, "Security in IoT layers: Emerging challenges with countermeasures," in *Computer Vision and Robotics: Proceedings of CVR 2022*: Springer, 2023, pp. 551-563.

[48] *IoT Architecture. Accessed: June. 22, 2025. [Online]*. Available: https://jelvix.com/blog/iot-architecture-layers

[49] R. Prakash, N. Jyoti, and S. Manjunatha, "A survey of security challenges, attacks in IoT," in *E3S Web of Conferences*, 2024, vol. 491, p. 04018: EDP Sciences.

[50] S. Abbas *et al.*, "Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks," vol. 10, p. e1793, 2024.

[51] M. Adam, M. Hammoudeh, R. Alrawashdeh, and B. J. I. A. Alsulaimy, "A Survey on Security, Privacy, Trust, and Architectural Challenges in IoT Systems," 2024.
[52] E. Altulaihan, M. A. Almaiah, and A. J. S. Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms," vol. 24, no. 2, p. 713, 2024.
[53] G. Agrawal, A. Kaur, and S. J. E. Myneni, "A Review of Generative Models in Generating Synthetic Attack Data for Cybersecurity," vol. 13, no. 2, p. 322, 2024.
[54] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in *2017 19th international conference on advanced communication technology (ICACT)*, 2017, pp. 464-467: IEEE.
[55] F. Pelekoudas-Oikonomou, J. C. Ribeiro, G. Mantas, G. Sakellari, and J. Gonzalez, "Prototyping a hyperledger fabric-based security architecture for IoMT-based health monitoring systems," *Future Internet*, vol. 15, no. 9, p. 308, 2023.
[56] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung, and J. H. J. E. Park, "Blockchain-based secure storage management with edge computing for IoT," vol. 8, no. 8, p. 828, 2019.
[57] V. T. Truong and L. B. Le, "MetaCIDS: Privacy-Preserving Collaborative Intrusion Detection for Metaverse based on Blockchain and Online Federated Learning," *IEEE Open Journal of the Computer Society*, 2023.
[58] A. Khang, V. Abdullayev, V. Hahanov, and V. Shah, *Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy*. CRC Press, 2024.
[59] M. Singh and S. Kim, "Trust bit: Reward-based intelligent vehicle commination using blockchain paper," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, 2018, pp. 62-67: IEEE.
[60] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. J. I. I. o. T. J. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," vol. 6, no. 2, pp. 2188-2204, 2018.
[61] Z. Ke and N. J. C. C. Park, "Performance modeling and analysis of Hyperledger Fabric," vol. 26, no. 5, pp. 2681-2699, 2023.
[62] K. Korpela, J. Hallikas, and T. Dahlberg, "Digital supply chain transformation toward blockchain integration," 2017.
[63] E. Blog, "On Public and Private Blockchains-Ethereum Blog.(2015)," ed, 2015.
[64] J. Yusoff, Z. Mohamad, M. J. J. o. C. Anuar, and Communications, "A review: Consensus algorithms on blockchain," vol. 10, no. 09, pp. 37-50, 2022.
[65] A. Tasdelen, "Fundamentals of Blockchain," in *Exploring Blockchain Applications*: CRC Press, 2024, pp. 6-25.
[66] M. I. Sarwar, L. A. Maghrabi, I. Khan, Q. H. Naith, and K. J. I. A. Nisar, "Blockchain: A Crypto-Intensive Technology-A Comprehensive Review," 2023.
[67] M. T. Hammi, B. Hammi, P. Bellot, A. J. C. Serhrouchni, and Security, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," vol. 78, pp. 126-142, 2018.
[68] M. Daghmehchi Firoozjaei, A. Ghorbani, H. Kim, and J. J. S. Song, "Hy-Bridge: A hybrid blockchain for privacy-preserving and trustful energy transactions in Internet-of-Things platforms," vol. 20, no. 3, p. 928, 2020.
[69] H. Xiong, T. Dalhaus, P. Wang, and J. J. f. i. B. Huang, "Blockchain technology for agriculture: applications and rationale," vol. 3, p. 7, 2020.
[70] P. Paul, P. Aithal, R. Saavedra, S. J. I. J. o. A. S. Ghosh, and Engineering, "Blockchain Technology and its Types—A Short Review," vol. 9, no. 2, pp. 189-200, 2021.
[71] I. A. Omar, R. Jayaraman, K. Salah, I. Yaqoob, S. J. A. J. f. S. Ellahham, and Engineering, "Applications of blockchain technology in clinical trials: review and open challenges," vol. 46, pp. 3001-3015, 2021.
[72] X. Yang, X. Li, H. Wu, and K. J. M. d. e. r. Zhao, "The application model and challenges of blockchain technology in education," vol. 2, pp. 34-45, 2017.
[73] B. Samuel and K. Kasturi, "A Review of Blockchain Technology in Smart Applications: Research Issues and Open Challenges," in *2023 International Conference on Computer Communication and Informatics (ICCCI)*, 2023, pp. 1-5: IEEE.
[74] G. Kaur and C. Gandhi, "Scalability in blockchain: Challenges and solutions," in *Handbook of Research on Blockchain Technology*: Elsevier, 2020, pp. 373-406.
[75] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. J. S. Puliafito, "Blockchain and iot integration: A systematic survey," vol. 18, no. 8, p. 2575, 2018.
[76] S. Asiri and A. Miri, "A sybil resistant IoT trust model using blockchains," in *2018 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)*, 2018, pp. 1017-1026: IEEE.
[77] A. Moinet, B. Darties, and J.-L. J. a. p. a. Baril, "Blockchain based trust & authentication for decentralized sensor networks," 2017.
[78] A. Singh, A. Smirti, R. Gupta, C. de Alwis, and A. Kalla, "Introduction to blockchain and smart contract–principles, applications, and security," in *Blockchain Technology in Healthcare Applications*: CRC Press, 2022, pp. 175-197.
[79] A. Sultan, M. A. Malik, and A. J. A. J. C. S. I. T. Mushtaq, "Internet of Things security issues and their solutions with blockchain technology characteristics: A systematic literature review," vol. 6, no. 3, p. 27, 2018.
[80] P. Xie, A. A. M. Kassim, M. Wei, R. A. A. J. J. o. S. Helmi, and M. Sciences, "Comprehensive Review of Blockchain Applications in Fintech Companies," vol. 14, no. 1, pp. 98-119, 2024.
[81] Y. J. J. o. I. I. I. Lu, "The blockchain: State-of-the-art and research challenges," vol. 15, pp. 80-90, 2019.
[82] S. Priyanka and A. J. I. J. S. R. S. E. T. Nagaratnam, "Blockchain evolution-a survey paper," vol. 4, no. 8, pp. 27-30, 2018.
[83] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. J. I. j. o. w. Wang, and g. services, "Blockchain challenges and opportunities: A survey," vol. 14, no. 4, pp. 352-375, 2018.
[84] L. Peng *et al.*, "Privacy preservation in permissionless blockchain: A survey," vol. 7, no. 3, pp. 295-307, 2021.
[85] R. J. J. o. H. M. Rajaguru and Management, "Effects of contemporary technologies, such as blockchain and artificial intelligence (AI) in enhancing consumers' trustworthiness of online reviews," vol. 33, no. 2, pp. 251-259, 2024.
[86] W. Fang *et al.*, "Digital signature scheme for information non-repudiation in blockchain: a state of the art review," vol. 2020, pp. 1-15, 2020.
[87] G. J. E. p. y. p. Wood. (2014, 2014). *Ethereum: A secure decentralised generalised transaction ledger Accessed: June. 22, 2025. [Online]*. . Available: https://files.gitter.im/ethereum/ yellowpaper/VIyt/Paper.pdf
[88] (29. Jan .2024). *Hyperledger Open Source Blockchain Technologies. Accessed: June. 22, 2025. [Online]* Available: https://www.hyperledger.org/
[89] *Multichain. Accessed: Accessed: June. 22, 2025. [Online]*. Available: https://www.multichain.com/
[90] *IOTA. Accessed: June. 22, 2025. [Online]*. Available: https://www.iota.org/
[91] *Corda. Accessed: June. 22, 2025. [Online]*. Available: https://r3.com/products/corda/
[92] M. I. Mehar *et al.*, "Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack," vol. 21, no. 1, pp. 19-32, 2019.
[93] S. Knezevic, "A blockchain approach for negotiating trust in IoT," 2020.

[94] A. Yewale, "Study of blockchain-as-a-service systems with a case study of hyperledger fabric implementation on Kubernetes," University of Nevada, Las Vegas, 2018.
[95] D. Li, W. E. Wong, and J. Guo, "A survey on blockchain for enterprise using hyperledger fabric and composer," in *2019 6th International Conference on Dependable Systems and Their Applications (DSA)*, 2020, pp. 71-80: IEEE.
[96] *Burrow. Accessed: June. 22, 2025. [Online]*. Available: https://www.hyperledger.org/projects/sawtooth
[97] T. Q. Ban, B. N. Anh, N. T. Son, and T. Van Dinh, "Survey of Hyperledger blockchain frameworks: case study in FPT university's cryptocurrency wallets," in *Proceedings of the 2019 8th International Conference on Software and Computer Applications*, 2019, pp. 472-480.
[98] V. Dhillon *et al.*, "The hyperledger project. Accessed: June. 22, 2025. Online]," pp. 139-149, 2017.
[99] *The Hyperledger greenhouse. Accessed: June. 22, 2025. [Online]*. Available: https://www.hyperledger.org/
[100] A. Rasti and A. Gheibi, "A Coin Marketplace Implementation on Blockchain Using the Hyperledger Platform," 2018.
[101] R. Gürfidan, M. J. J. o. D. Ersoy, Information, and Management, "A new approach with blockchain based for safe communication in IoT ecosystem," vol. 4, no. 1, pp. 49-56, 2022.
[102] *Waltonchain. Accessed: June. 22, 2025. [Online]*. Available: https://www.waltonchain.org/
[103] C. Saraf and S. Sabadra, "Blockchain platforms: A compendium," in *2018 IEEE International Conference on Innovative Research and Development (ICIRD)*, 2018, pp. 1-6: IEEE.
[104] S. Dalla Palma, R. Pareschi, and F. Zappone, "What is your distributed (hyper) ledger?," in *2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, 2021, pp. 27-33: IEEE.
[105] A. Abdelmaboud *et al.*, "Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions," vol. 11, no. 4, p. 630, 2022.
[106] S. Nikolić, N. Zdravković, I. Franc, and N. Arivazhagan, "A Comparison on Hyperledger Consensus Mechanism Security and their Applications," 2023.
[107] *Cardano. Accessed: June. 22, 2025. [Online]*. Available: https://www.cardano.org/en/home/
[12] (Sep. 2019). Iota. [
[108] C. Fan, C. Lin, H. Khazaei, and P. Musilek, "Performance analysis of hyperledger besu in private blockchain," in *2022 IEEE international conference on decentralized applications and infrastructures (DAPPS)*, 2022, pp. 64-73: IEEE.
[109] M. S. Ferdous, K. Biswas, M. J. M. Chowdhury, N. Chowdhury, and V. Muthukkumarasamy, "Integrated platforms for blockchain enablement," in *Advances in Computers*, vol. 115: Elsevier, 2019, pp. 41-72.
[110] G. J. A. J. Gideon, "Multichain Private Blockchain White Paper," vol. 28, p. 2021, 2015.
[111] M. J. M. Chowdhury *et al.*, "A comparative analysis of distributed ledger technology platforms," vol. 7, pp. 167930-167943, 2019.
[112] S. J. W. p. Popov, "The tangle," vol. 1, no. 3, p. 30, 2018.
[113] R. Brown, "The Corda platform: An introduction white paper," 2018.
[114] D. Schwartz, N. Youngs, and A. J. R. L. I. W. P. Britto, "The ripple protocol consensus algorithm Accessed: June. 22, 2025. [Online]. ," vol. 5, no. 8, p. 151, 2014.
[115] H. Team, "HDAC: transaction innovation—IoT contract M2M transaction platform based on blockchain," ed, 2018.
[116] J. Kwon and E. J. U. h. c. n. w. Buchman, "Cosmos: A network of distributed ledgers," 2016.
[117] I. J. I. T. Team, "IoTeX: a decentralized network for Internet of Things powered by a privacy-centric blockchain," 2018.
[118] T. McConaghy *et al.*, "Bigchaindb: a scalable blockchain database," pp. 53-72, 2016.
[119] R. Creighton, "Domus Tower Blockchain (DRAFT) March 28, 2016," 2016.
[120] *HydraChain. Accessed: June. 22, 2025. [Online]*. Available: https://github.com/HydraChain
[121] *Openchain Blockchain Technology for the Enterprise. Accessed: June. 22, 2025. [Online]*. Available: https://www.openchain.org/
[122] *Eos. Accessed: June. 22, 2025. [Online]*. Available: https://eos.io/
[123] P. Grover, A. K. Kar, M. Janssen, and P. V. J. E. I. S. Ilavarasan, "Perceived usefulness, ease of use and user acceptance of blockchain technology for digital transactions–insights from user-generated content on Twitter," vol. 13, no. 6, pp. 771-800, 2019.
[124] B. J. I. S. Anthony Jr, "Distributed ledger and decentralised technology adoption for smart digital transition in collaborative enterprise. Enterp," pp. 1-34, 2021.
[125] S. Cherbal, A. Zier, S. Hebal, L. Louail, and B. J. T. J. o. S. Annane, "Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing," vol. 80, no. 3, pp. 3738-3816, 2024.
[126] H. Moudoud, S. Cherkaoui, and L. Khoukhi, "An IoT blockchain architecture using oracles and smart contracts: the use-case of a food supply chain," in *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2019, pp. 1-6: IEEE.
[127] S. Biswas, K. Sharif, F. Li, S. Maharjan, S. P. Mohanty, and Y. J. I. I. o. T. J. Wang, "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," vol. 7, no. 3, pp. 2343-2355, 2019.
[128] R. Boncea, I. Petre, and V. J. R. C. S. J. Vevera, "Building trust among things in omniscient Internet using Blockchain Technology," vol. 1, no. 1, pp. 17-24, 2019.
[129] A. Reyna, C. Martín, J. Chen, E. Soler, and M. J. F. g. c. s. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," vol. 88, pp. 173-190, 2018.
[130] L. J. C. A. a. h. w. c. c. a. w.-a.-s.-c.-a.-h.-d.-i.-w. h. Mearian, "What'sa smart contract (and how does it work)," 2019.
[131] Y. Zhou, R. Han, and Y. J. E. Li, "Reputation consensus mechanism for blockchain based on information-centric networking," vol. 14, no. 6, p. 1099, 2025.
[132] I. A. Reshi and S. J. C. C. Sholla, "IBF network: enhancing network privacy with IoT, blockchain, and fog computing on different consensus mechanisms," vol. 28, no. 3, p. 208, 2025.
[133] N. Ilakkiya and A. Rajaram, "Blockchain-Enabled Lightweight Intrusion Detection System for Secure MANETs," *Journal of Electrical Engineering & Technology*, pp. 1-15, 2024.
[134] N. Alsaeed, F. Nadeem, and F. J. F. G. C. S. Albalwy, "A scalable and lightweight group authentication framework for Internet of Medical Things using integrated blockchain and fog computing," vol. 151, pp. 162-181, 2024.
[135] P. Bhattacharya *et al.*, "LightBlocks: A trusted lightweight signcryption and consensus scheme for industrial IoT ecosystems," vol. 88, p. 103785, 2024.
[136] X. Zhou *et al.*, "Federated distillation and blockchain empowered secure knowledge sharing for Internet of medical Things," vol. 662, p. 120217, 2024.
[137] Z. WANG, J. Li, A. Liu, K. Ota, M. Dong, and X. Chen, "RQPoA: A random quantum PoA Consensus Mechanism in Blockchain Based on Quantum Methods," 2024.
[138] R. Huang, X. Yang, P. J. I. o. T. Ajay, and C.-P. Systems, "Consensus mechanism for software-defined blockchain in internet of things," vol. 3, pp. 52-60, 2023.

[139] Y. Zhao, Y. Qu, Y. Xiang, Y. Zhang, and L. J. I. T. o. S. C. Gao, "A Lightweight Model-Based Evolutionary Consensus Protocol in Blockchain as a Service for IoT," 2023.
[140] A. Dorri and R. Jurdak, "Tree-chain: A fast lightweight consensus algorithm for iot applications," in *2020 IEEE 45th Conference on Local Computer Networks (LCN)*, 2020, pp. 369-372: IEEE.
[141] G. Shi *et al.*, "MEDACCESSX: A Blockchain-Enabled Dynamic Access Control Framework for IoMT Networks," vol. 25, no. 6, p. 1857, 2025.
[142] G. Piao, J. J. P.-t.-P. N. Zhu, and Applications, "AccessChain: A scalable and privacy-preserving access control scheme for blockchain-based IoT," vol. 18, no. 2, p. 92, 2025.
[143] E. A. Shammar, A. T. Zahary, A. A. J. W. C. Al-Shargabi, and M. Computing, "An attribute-based access control model for Internet of Things using hyperledger fabric blockchain," vol. 2022, no. 1, p. 6926408, 2022.
[144] P. Li, D. Zhou, H. Ma, and J. J. J. o. S. A. Lai, "Flexible and secure access control for EHR sharing based on blockchain," vol. 146, p. 103033, 2024.
[145] M. Khalid, S. Hameed, A. Qadir, S. A. Shah, and D. J. C. C. Draheim, "Towards SDN-based smart contract solution for IoT access control," vol. 198, pp. 1-31, 2023.
[146] S. Kaven and V. Skwarek, "Poster: Attribute based access control for IoT devices in 5G networks," in *Proceedings of the 28th ACM Symposium on Access Control Models and Technologies*, 2023, pp. 51-53.
[147] S. Algarni *et al.*, "Blockchain-based secured access control in an IoT system," vol. 11, no. 4, p. 1772, 2021.
[148] R. Muñoz *et al.*, "Integration of IoT, transport SDN, and edge/cloud computing for dynamic distribution of IoT analytics and efficient use of network resources," vol. 36, no. 7, pp. 1420-1428, 2018.
[149] R. Sethi, B. Bhushan, N. Sharma, R. Kumar, and I. J. M. t. i. t. I. o. T. e. Kaushik, "Applicability of industrial IoT in diversified sectors: evolution, applications and challenges," pp. 45-67, 2021.
[150] A. Malik, S. Gautam, S. Abidin, and B. Bhushan, "Blockchain technology-future of IoT: including structure, limitations and various possible attacks," in *2019 2nd international conference on intelligent computing, instrumentation and control technologies (ICICICT)*, 2019, vol. 1, pp. 1100-1104: IEEE.
[151] W. Pan, F. Zheng, Y. Zhao, W.-T. Zhu, J. J. I. T. o. I. F. Jing, and Security, "An efficient elliptic curve cryptography signature server with GPU acceleration," vol. 12, no. 1, pp. 111-122, 2016.
[152] J. Wu, F. Xiong, and C. J. I. A. Li, "Application of Internet of Things and blockchain technologies to improve accounting information quality," vol. 7, pp. 100090-100098, 2019.
[153] A. Al Sadawi, M. S. Hassan, and M. J. I. A. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," vol. 9, pp. 54478-54497, 2021.
[154] C. Lin, D. He, X. Huang, K.-K. R. Choo, A. V. J. J. o. n. Vasilakos, and c. applications, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," vol. 116, pp. 42-52, 2018.
[155] S. Wang, D. Li, Y. Zhang, and J. J. I. a. Chen, "Smart contract-based product traceability system in the supply chain scenario," vol. 7, pp. 115122-115133, 2019.
[156] C. Kolias, G. Kambourakis, A. Stavrou, and J. J. C. Voas, "DDoS in the IoT: Mirai and other botnets," vol. 50, no. 7, pp. 80-84, 2017.
[157] S. Sicari, A. Rizzardi, D. Miorandi, and A. J. C. N. Coen-Porisini, "REATO: REActing TO Denial of Service attacks in the Internet of Things," vol. 137, pp. 37-48, 2018.
[158] H. Halpin and M. Piekarska, "Introduction to Security and Privacy on the Blockchain," in *2017 IEEE European symposium on security and privacy workshops (EuroS&PW)*, 2017, pp. 1-3: IEEE.
[159] A. M. Almasabi, A. B. Alkhodre, M. Khemakhem, F. Eassa, A. A. Abi Sen, and A. J. I. Harbaoui, "Internet of Things-Based Anomaly Detection Hybrid Framework Simulation Integration of Deep Learning and Blockchain," vol. 16, no. 5, p. 406, 2025.
[160] D. JYOTHI *et al.*, "DESIGN OF AN IMPROVED METHOD FOR INTRUSION DETECTION USING CNN, LSTM, AND BLOCK CHAIN," vol. 102, no. 1, 2025.
[161] E. Ntizikira, L. Wang, J. Chen, and K. Saleem, "Honey-block: Edge assisted ensemble learning model for intrusion detection and prevention using defense mechanism in IoT," *Computer Communications*, vol. 214, pp. 1-17, 2024.
[162] V. T. Truong and L. B. Le, "Security for the Metaverse: Blockchain and Machine Learning Techniques for Intrusion Detection," *IEEE Network*, 2024.
[163] R. Hanumantharaju, K. Shreenath, B. Sowmya, and K. Srinivasa, "Fog-Driven Approach for Distributed Intrusion Detection System in Auditing the Data Dased on Blockchain-Cloud Systems," *Cloud Computing and Data Science*, pp. 97-107, 2024.
[164] N. Sun, W. Wang, Y. Tong, and K. J. F. o. C. S. Liu, "Blockchain based federated learning for intrusion detection for Internet of Things," vol. 18, no. 5, p. 185328, 2024.
[165] S.-J. Hsiao and W.-T. Sung, "Enhancing cybersecurity using blockchain technology based on IoT data fusion," *IEEE Internet of Things Journal*, vol. 10, no. 1, pp. 486-498, 2022.
[166] I. Aliyu, M. C. Feliciano, S. Van Engelenburg, D. O. Kim, and C. G. Lim, "A blockchain-based federated forest for SDN-enabled in-vehicle network intrusion detection system," *IEEE Access*, vol. 9, pp. 102593-102608, 2021.
[167] W. Li, Y. Wang, J. Li, and M. H. Au, "Toward a blockchain-based framework for challenge-based collaborative intrusion detection," *International Journal of Information Security*, vol. 20, pp. 127-139, 2021.
[168] M. Iqbal, A. Kormiltsyn, V. Dwivedi, and R. Matulevičius, "Blockchain-based ontology driven reference framework for security risk management," *Data & Knowledge Engineering*, vol. 149, p. 102257, 2024.
[169] A. Cirne, P. R. Sousa, J. S. Resende, and L. Antunes, "Hardware security for Internet of Things identity assurance," *IEEE Communications Surveys & Tutorials*, 2024.
[170] S. M. Othman, A. Y. Al-mutawkkil, A. M. J. S. a. U. J. o. A. S. Alnashi, and Technology, "Survey of Intrusion Detection Techniques in Cloud Computing," vol. 2, no. 4, pp. 363-374, 2024.
[171] M. Ghurab, G. Gaphari, F. Alshami, R. Alshamy, and S. J. A. J. o. R. i. C. S. Othman, "A detailed analysis of benchmark datasets for network intrusion detection system," vol. 7, no. 4, pp. 14-33, 2021.
[172] B. Kaur *et al.*, "Internet of things (IoT) security dataset evolution: Challenges and future directions," p. 100780, 2023.
[173] (2024). *CICIoMT2024 Dataset. Accessed: June. 22, 2025. [Online]*. Available: https://www.unb.ca/cic/datasets/iomt-dataset-2024.html
[174] P. Chandekar, M. Mehta, and S. J. a. p. a. Chandan, "Enhanced anomaly detection in iomt networks using ensemble ai models on the ciciomt2024 dataset," 2025.
[175] J. Domènech, O. León, M. S. Siddiqui, and J. J. I. o. T. Pegueroles, "Evaluating and enhancing intrusion detection systems in IoMT: The importance of domain-specific datasets," p. 101631, 2025.
[176] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani. (2023). *CIC IoT Attack Dataset 2023 [Online]*. Available: https://www.unb.ca/cic/datasets/iotdataset-2023.html

[177] Q. Gulzar, K. J. I. J. o. M. L. Mustafa, and Cybernetics, "Enhancing network security in industrial IoT environments: a DeepCLG hybrid learning model for cyberattack detection," pp. 1-19, 2025.

[178] A. M. Al-Ghamdi and M. M. J. I. I. J. o. C. S. Alansari, "Enhancing IoT Security: A Comparative Study of CNN and RNN-Based Anomaly Detection Using the CICIoT2023 Dataset," vol. 52, no. 5, 2025.

[179] Y. Kim, S. Hakak, and A. Ghorbani. (2023 ). *DDoS Attack (CICEV2023). Accessed: June. 22, 2025. [Online]*. Available: https://www.unb.ca/cic/datasets/cicev2023.html

[180] F. M. Talaat, M. M. E. Khoudier, I. F. Moawad, and A. El-Ghamry, "Fortifying EV Charging Stations: AI-Powered Detection and Mitigation of DDoS Attacks Using Personalized Federated Learning."

[181] A. G. Kumar and S. Dahiya, "Machine Learning for Advancing Electric Vehicles Security Leveraging CICEVSE2024," in *2025 International Russian Smart Industry Conference (SmartIndustryCon)*, 2025, pp. 240-245: IEEE.

[182] S. Dadkhah, H. Mahdikhani, P. K. Danso, A. Zohourian, K. A. Truong, and A. A. Ghorbani. (2022). *CIC IoT Dataset 2022 [Online]*. Available: https://www.unb.ca/cic/datasets/iotdataset-2022.htmll

[183] H. Wasswa, H. Abbass, and T. J. A. a. S. Lynar, "Latent Space Alignment for Robust Detection of Iot Botnet Attacks in Non-Stationary Environments."

[184] M. Rabbani *et al.*, "A lightweight IoT device identification using enhanced behavioral-based features," vol. 18, no. 2, pp. 1-22, 2025.

[185] H. Hindy, C. Tachtatzis, R. Atkinson, E. Bayne, and X. J. D. h. d. o. b.-e. Bellekens, "MQTT-IOT-IDS2020: MQTT internet of things intrusion detection dataset (2020)," 2020.

[186] H. Zeghida *et al.*, "Enhancing IoT cyber attacks intrusion detection through GAN-based data augmentation and hybrid deep learning models for MQTT network protocol cyber attacks," vol. 28, no. 1, p. 58, 2025.

[187] H. Zeghida, M. Boulaiche, R. Chikh, A. Patel, A. L. B. Barros, and A. M. J. I. J. o. I. S. Bamhdi, "XMID-MQTT: explaining machine learning-based intrusion detection system for MQTT protocol in IoT environment," vol. 24, no. 3, pp. 1-22, 2025.

[188] (2020). *The BoT-IoT Dataset. Accessed: June. 22, 2025. [Online]*. Available: https://ieee-dataport.org/documents/bot-iot-dataset#files

[189] M. Luqman *et al.*, "Intelligent parameter-based in-network IDS for IoT using UNSW-NB15 and BoT-IoT datasets," vol. 362, no. 1, p. 107440, 2025.

[190] J. Ashraf, G. M. Raza, B.-S. Kim, A. Wahid, and H.-Y. J. A. S. Kim, "Making a Real-Time IoT Network Intrusion-Detection System (INIDS) Using a Realistic BoT–IoT Dataset with Multiple Machine-Learning Classifiers," vol. 15, no. 4, 2025.

[191] N. Kumaran, S. M. J. C. JS, and SYSTEMS, "BRDO: Blockchain Assisted Intrusion Detection Using Optimized Deep Stacked Network," 2023.

[192] T. Sharma, U. J. I. J. o. A. R. Datta, and M. Trends, "An Intelligent Intrusion Detection Using Deep Learning on CICIDS2018 for Cloud Security," vol. 2, no. 2, pp. 747-759, 2025.

[193] Q. M. Alzubi, S. N. Makhadmeh, and Y. J. J. o. A. i. I. T. Sanjalawe, "Optimizing Intrusion Detection: Advanced Feature Selection and Machine Learning Techniques Using the CSE-CIC-IDS2018 Dataset," vol. 16, no. 3, 2025.

[194] G. S. C. Kumar, R. K. Kumar, K. P. V. Kumar, N. R. Sai, and M. J. E. S. w. A. Brahmaiah, "Deep residual convolutional neural Network: An efficient technique for intrusion detection system," vol. 238, p. 121912, 2024.

[195] M. Ali, S. Pervez, S. E. Hosseini, M. K. J. I. J. o. O. Siddhu, and B. Engineering, "Evaluation and Detection of Cyberattack in IoT-Based Smart City Networks Using Machine Learning on the UNSW-NB15 Dataset," vol. 21, no. 2, 2025.

[196] V. Kumar, V. Kumar, A. P. S. Bhadauria, J. Dixit, and A. Kumar, "Intrusion Detection at the Edge Computing: A Deep Learning Approach Using the UNSW-NB15 Dataset," in *2025 IEEE 14th International Conference on Communication Systems and Network Technologies (CSNT)*, 2025, pp. 220-224: IEEE.

[197] "ISCX2012 dataset. Accessed: 2012 [Online].", ed.

[198] S. Ahmadi, "Evolving Botnet Defenses: A Survey of Machine Learning Approaches for Identifying Polymorphic and Evasive Malware," 2025.

[199] S. Vadlamudi and A. V. Bharathy, "Systematic Study on AI-Enabled Defense Against DDoS Attacks in IoT," in *2025 International Conference on Intelligent Systems and Computational Networks (ICISCN)*, 2025, pp. 1-7: IEEE.

[200] S. Bindra, A. Malik, and S. Singh, "Improving Intrusion Detection for IoT Networks Using SMOTE and PCA on NSL-KDD Dataset," in *2025 3rd International Conference on Disruptive Technologies (ICDT)*, 2025, pp. 1623-1628: IEEE.

[201] R. Alshamy, M. J. I. J. o. C. N. AKCAYOL, and Communications, "INTRUSION DETECTION MODEL USING MACHINE LEARNING ALGORITHMS ON NSL-KDD DATASET," vol. 16, no. 6, 2024.

[202] B. Lampe and W. Meng, "can-train-and-test: A New CAN Intrusion Detection Dataset," in *2023 IEEE 98th Vehicular Technology Conference (VTC2023-Fall)*, 2023, pp. 1-7: IEEE.

[203] (2024). *CICIoV2024. Accessed: June. 22, 2025. [Online]*. Available: https://www.unb.ca/cic/datasets/iov-dataset-2024.html

[204] H. Lee, S. H. Jeong, and H. K. Kim, "OTIDS: A novel intrusion detection system for in-vehicle network by using remote frame," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, 2017, pp. 57-5709: IEEE.

[205] M. L. Han, B. I. Kwak, and H. K. Kim, "Anomaly intrusion detection method for vehicular networks based on survival analysis," *Vehicular communications*, vol. 14, pp. 52-63, 2018.

[206] C. Kaiser, A. Stocker, and A. Festl, "Automotive CAN bus data: an example dataset from the AEGIS big data project. Zenodo," ed, 2019.

[207] H. M. Song and H. K. Kim, "Discovering can specification using on-board diagnostics," *IEEE Design & Test*, vol. 38, no. 3, pp. 93-103, 2020.

[208] H. Kang, B. I. Kwak, Y. H. Lee, H. Lee, H. Lee, and H. K. Kim, "Car hacking and defense competition on in-vehicle network," in *Workshop on Automotive and Autonomous Vehicle Security (AutoSec)*, 2021, vol. 2021, p. 25.

[209] U. o. Turku. (2021). *Can bus dataset collected from a heavy-duty truck Fairdata , . [Online]. .* Available: https://etsin.fairdata.fi/dataset/7586f24f-c91b-41df-92af-283524de8b3e

[210] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd international conference on open and big data (OBD)*, 2016, pp. 25-30: IEEE.

[211] L. A. Linn and M. B. Koo, "Blockchain for health data and its potential use in health it and health care related research," in *ONC/NIST use of blockchain for healthcare and research workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016, pp. 1-10.

[212] A. Tumasjan, "The promise and prospects of blockchain-based decentralized business models," in *Knowledge and digital technology*: Springer Nature Switzerland Cham, 2024, pp. 203-224.

[213] N. J. D. B. Upadhyay, "Business models for the Blockchain: An empirical analysis," p. 100082, 2024.

[214] S. Schneider, M. Leyer, and M. J. I. T. o. E. M. Tate, "The transformational impact of blockchain technology on business models and ecosystems: A symbiosis of human and technology agents," vol. 67, no. 4, pp. 1184-1195, 2020.

[215] T. L. N. Dang and M. S. Nguyen, "An approach to data privacy in smart home using blockchain technology," in *2018 International Conference on Advanced Computing and Applications (ACOMP)*, 2018, pp. 58-64: IEEE.

[216] A. Qashlan, P. Nanda, X. He, and M. J. I. A. Mohanty, "Privacy-preserving mechanism in smart home using blockchain," vol. 9, pp. 103651-103669, 2021.

[217] F. Sabrina, "Blockchain and structural relationship based access control for IoT: a smart city use case," in *2019 IEEE 44th Conference on Local Computer Networks (LCN)*, 2019, pp. 137-140: IEEE.
[218] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, W. J. I. c. s. Ni, and tutorials, "Anatomy of threats to the internet of things," vol. 21, no. 2, pp. 1636-1675, 2018.
[219] S. Hakak, W. Z. Khan, G. A. Gilkar, M. Imran, and N. J. I. N. Guizani, "Securing smart cities through blockchain technology: Architecture, requirements, and challenges," vol. 34, no. 1, pp. 8-14, 2020.
[220] N. Ullah, W. Mugahed Al-Rahmi, A. I. Alzahrani, O. Alfarraj, and F. M. J. S. Alblehai, "Blockchain technology adoption in smart learning environments," vol. 13, no. 4, p. 1801, 2021.
[221] P. Bhaskar, C. K. Tiwari, A. J. I. T. Joshi, and S. Education, "Blockchain in education management: present and future applications," vol. 18, no. 1, pp. 1-17, 2021.
[222] U. Eaganathan, V. V. Indrian, and Y. Nathan, "Ideation framework of block chain adoption in Malaysia higher education," in *Journal of Physics: Conference Series*, 2019, vol. 1228, no. 1, p. 012072: IOP Publishing.
[223] M. Gottlieb, C. Deutsch, F. Hoops, H. Pongratz, H. J. B. R. Krcmar, and Applications, "Expedition to the Blockchain Application Potential for Higher Education Institutions," p. 100203, 2024.
[224] A. Z. Al-Marridi, A. Mohamed, A. J. J. o. N. Erbad, and C. Applications, "Optimized blockchain-based healthcare framework empowered by mixed multi-agent reinforcement learning," vol. 224, p. 103834, 2024.
[225] R. Dahiya *et al.*, "A Blockchain Based Security system framework in Healthcare Domain using IoT," vol. 20, no. 3s, pp. 2039-2050, 2024.
[226] C. Prybila, S. Schulte, C. Hochreiner, and I. J. F. g. c. s. Weber, "Runtime verification for business processes utilizing the Bitcoin blockchain," vol. 107, pp. 816-831, 2020.
[227] A. Tchagna Kouanou *et al.*, "Securing data in an internet of things network using blockchain technology: smart home case," vol. 3, no. 2, p. 167, 2022.
[228] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, 2017, pp. 618-623: IEEE.
[229] A. Di Vaio and L. J. I. J. o. I. M. Varriale, "Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry," vol. 52, p. 102014, 2020.
[230] Z. Liu and Z. J. I. j. o. i. m. Li, "A blockchain-based framework of cross-border e-commerce supply chain," vol. 52, p. 102059, 2020.
[231] S. Yadav, S. P. J. R. Singh, Conservation, and Recycling, "Blockchain critical success factors for sustainable supply chain," vol. 152, p. 104505, 2020.
[232] K. S. Divya *et al.*, "Implementing Blockchain Based DApp for Secure Sharing of Students' Credentials," in *2024 IEEE 9th International Conference for Convergence in Technology (I2CT)*, 2024, pp. 1-6: IEEE.
[233] G. Bjelobaba, A. Savić, T. Tošić, I. Stefanović, and B. J. S. Kocić, "Collaborative learning supported by Blockchain Technology as a model for improving the Educational process," vol. 15, no. 6, p. 4780, 2023.
[234] A. Odeh and A. J. A. S. Abu Taleb, "Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection," vol. 13, no. 21, p. 11985, 2023.
[235] K. N. Lawal, T. K. Olaniyi, and R. M. J. A. S. Gibson, "Leveraging Real-World Data from IoT Devices in a Fog–Cloud Architecture for Resource Optimisation within a Smart Building," vol. 14, no. 1, p. 316, 2023.
[236] P. Sethi, S. R. J. J. o. e. Sarangi, and c. engineering, "Internet of things: architectures, protocols, and applications," vol. 2017, no. 1, p. 9324035, 2017.
[237] R. Porkodi and V. Bhuvaneswari, "The internet of things (IOT) applications and communication enabling technology standards: An overview," in *2014 International conference on intelligent computing applications*, 2014, pp. 324-329: IEEE.
[238] C. Sarkar, S. A. U. Nambi, R. V. Prasad, and A. Rahim, "A scalable distributed architecture towards unifying IoT applications," in *2014 IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 508-513: IEEE.
[239] M. Noaman, M. S. Khan, M. F. Abrar, S. Ali, A. Alvi, and M. A. J. S. P. Saleem, "Challenges in integration of heterogeneous internet of things," vol. 2022, no. 1, p. 8626882, 2022.
[240] M. Mukherjee, L. Shu, D. J. I. C. S. Wang, and Tutorials, "Survey of fog computing: Fundamental, network applications, and research challenges," vol. 20, no. 3, pp. 1826-1857, 2018.
[241] C. Sabri, L. Kriaa, and S. L. Azzouz, "Comparison of IoT constrained devices operating systems: A survey," in *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, 2017, pp. 369-375: IEEE.
[242] M. A. Musarat, W. S. Alaloul, A. M. Khan, S. Ayub, and N. J. R. i. E. Jousseaume, "A survey-based approach of framework development for improving the application of internet of things in the construction industry of Malaysia," p. 101823, 2024.
[243] H. Kuchuk and E. J. A. I. S. Malokhvii, "INTEGRATION OF IOT WITH CLOUD, FOG, AND EDGE COMPUTING: A REVIEW," vol. 8, no. 2, pp. 65-78, 2024.
[244] S. Li, L. D. Xu, and S. J. I. s. f. Zhao, "The internet of things: a survey," vol. 17, pp. 243-259, 2015.
[245] H. J. S. J. B. L. Hughes and Pol'y, "Blockchain and the future of secured transactions law," vol. 3, p. 21, 2020.
[246] E. J. B. Ganne, Big Data and C. Global Trade Law, "Blockchain's Practical and Legal Implications for Global Trade and Global Trade Law," pp. 128-159, 2021.
[247] A. Bhattacharjya, X. Zhong, J. Wang, X. J. C.-P. S. a. Li, security, and application, "Security challenges and concerns of Internet of Things (IoT)," pp. 153-185, 2019.
[248] S. Quincozes, T. Emilio, and J. J. I. L. A. T. Kazienko, "MQTT protocol: fundamentals, tools and future directions," vol. 17, no. 09, pp. 1439-1448, 2019.
[249] Y. Liu, J. Zhang, and J. J. C. C. Zhan, "Privacy protection for fog computing and the internet of things data based on blockchain," vol. 24, no. 2, pp. 1331-1345, 2021.
[250] E. Fazel, M. Z. Nezhad, J. Rezazadeh, M. Moradi, and J. J. I. o. T. Ayoade, "IoT convergence with machine learning & blockchain: A review," p. 101187, 2024.
[251] J. Andrew *et al.*, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," vol. 215, p. 103633, 2023.
[252] I. Fathail and V. D. Bhagile, "IoT based machine learning techniques for healthcare applications," in *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*, 2020, pp. 248-252: IEEE.
[253] F. Girardi, G. De Gennaro, L. Colizzi, and N. J. E. Convertini, "Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain," vol. 9, no. 6, p. 884, 2020.
[254] D. V. J. H. i. r. Dimitrov, "Medical internet of things and big data in healthcare," vol. 22, no. 3, pp. 156-163, 2016.
[255] M. J. G. D. o. E. Manavalan and Business, "Intersection of artificial intelligence, machine learning, and internet of things–an economic overview," vol. 9, no. 2, pp. 119-128, 2020.

[256] D. Bacciu, S. Chessa, C. Gallicchio, and A. Micheli, "On the need of machine learning as a service for the internet of things," in *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, 2017, pp. 1-8.
[257] Y. B. Zikria, M. K. Afzal, S. W. Kim, A. Marin, and M. J. C. C. Guizani, "Deep learning for intelligent IoT: Opportunities, challenges and solutions," vol. 164, ed: Elsevier, 2020, pp. 50-53.
[258] A. Rahman *et al.*, "Smartblock-sdn: An optimized blockchain-sdn framework for resource management in iot," vol. 9, pp. 28361-28376, 2022.
[259] S. Rathore, B. W. Kwon, J. H. J. J. o. N. Park, and C. Applications, "BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network," vol. 143, pp. 167-177, 2019.
[260] H. Zhou, C. She, Y. Deng, M. Dohler, and A. J. I. W. C. Nallanathan, "Machine learning for massive industrial internet of things," vol. 28, no. 4, pp. 81-87, 2023.
[261] E. Münsing, J. Mather, and S. Moura, "Blockchains for decentralized optimization of energy resources in microgrid networks," in *2017 IEEE conference on control technology and applications (CCTA)*, 2019, pp. 2164-2171: IEEE.
[262] A. Aljabri, F. Jemili, O. J. I. J. o. C. Korbaa, and Applications, "Convolutional neural network for intrusion detection using blockchain technology," vol. 46, no. 2, pp. 67-77, 2024.
[263] K. Venkatesan and S. B. J. S. R. Rahayu, "Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques," vol. 14, no. 1, p. 1149, 2024.
[264] Y. Djenouri, G. Srivastava, A. Belhadi, and J. C. W. J. T. o. E. T. T. Lin, "Intelligent blockchain management for distributed knowledge graphs in IoT 5G environments," vol. 35, no. 4, p. e4332, 2024.
[265] B. Bordel, P. Lebigot, R. Alcarria, and T. Robles, "Digital food product traceability: using blockchain in the international commerce," in *Digital Science*, 2019, pp. 224-231: Springer.
[266] D. J. A. A. t. S. Azimov, Business, Innovation in Digital Economy, "Analysis of the international experience of implementing blockchain technology," vol. 2, no. 2, pp. 138-149, 2021.
[267] A. Hooper, D. J. R. o. I. B. Holtbrügge, and Strategy, "Blockchain technology in international business: changing the agenda for global governance," vol. 30, no. 2, pp. 183-200, 2020.