Computer Standards & Interfaces 96 (2026) 104068

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Reliability techniques and architectures for blockchain-enabled internet of things: Current applications, systematic review, and future trends

Xin Sun [a], Xinglong Yu [a,*], Qinlu Huang [a], Zhigang Wang [b,c,*], Jiahu Guo [b,d], Zhihao Huang [c], Fei Xie [c]

[a] School of Electrical and Information Engineering, Chengdu Textile College, Chengdu 611731, China
[b] Emergency Management College, Chengdu University, Chengdu 610106, China
[c] Zhi Fei Space (Chengdu) Information Technology Co., Ltd., Chengdu 610083, China
[d] Major Hazard Monitoring and Emergency Response Key Laboratory of Sichuan Province, Chengdu 610106, China

ARTICLE INFO

Keywords:
Internet of things
Blockchain
Lightweight
Security
Fault-Tolerant
Data integrity

ABSTRACT

The rapid proliferation of Internet of Things (IoT) devices across diverse sectors has amplified concerns regarding security, scalability, and trust, particularly due to the reliance on centralized architectures. Blockchain, with its decentralized structure and cryptographic foundations, has emerged as a potential enabler of secure, scalable, and accountable IoT ecosystems. Despite increasing interest, limited attention has been paid to the reliability and dependability mechanisms in blockchain-enabled IoT networks, especially in resource-constrained or developing regions. This study presents a systematic review of key publications, categorizing them into five principal groups: consensus mechanisms, fault-tolerant designs, data integrity techniques, multi-tier-based mechanisms, and lightweight blockchain-based mechanisms. By employing this taxonomy, the review investigates how different technical approaches ranging from advanced cryptography methods to symmetry-based architectural designs contribute to trust management, operational resilience, and data protection in IoT ecosystems. The findings suggest that although blockchain integration holds substantial potential for overcoming existing limitations in IoT infrastructures, it also presents new engineering and architectural challenges. Nevertheless, the diverse techniques identified in the literature demonstrate tangible progress in improving efficiency, reducing latency, and enhancing the overall reliability and security of decentralized IoT networks.

1. Introduction

The Internet of Things (IoT), initially introduced by Ashton in 1999, refers to a network of interconnected physical devices capable of data collection and communication through technologies such as Radio Frequency Identification (RFID) [1,2]. Over time, the concept has evolved across disciplines, linking the physical and virtual worlds through billions of connected devices [3]. IoT has seen rapid growth, now outnumbering the global human population, and has been widely adopted in domains including smart cities, healthcare, environmental monitoring, and transportation systems due to its scalability and ease of deployment [4]. However, the increasing scale and heterogeneity of IoT systems also introduce significant challenges, such as data interoperability, system scalability, and secure device communication [5,6].

A primary concern in traditional IoT architecture is the reliance on centralized servers or cloud infrastructures for control and data processing. This centralized model presents vulnerabilities such as single points of failure, potential misuse of user data, and performance bottlenecks due to geographic distance between devices and servers [7,8]. Furthermore, IoT devices frequently transmit sensitive personal data, heightening privacy concerns and necessitating robust mechanisms for data protection [9,10]. As a response to these limitations, researchers are increasingly advocating for decentralized frameworks that minimize trust dependencies and mitigate centralized risks.

Blockchain technology has emerged as a viable decentralized solution for enhancing IoT security and reliability. As a peer-to-peer distributed ledger, blockchain maintains immutable transaction records validated through consensus mechanisms such as Proof of Work (PoW) or Practical Byzantine Fault Tolerance (PBFT) [11–13]. The use of smart contracts further expands blockchain's utility by enabling automated, tamper-proof execution of predefined logic [14]. Additionally, digital signatures, cryptography, and cryptographic hashes ensure

* Corresponding authors.
E-mail addresses: yuxl@cdtc.edu.cn (X. Yu), wangzhigang@cdu.edu.cn (Z. Wang).

https://doi.org/10.1016/j.csi.2025.104068
Received 24 December 2024; Received in revised form 22 August 2025; Accepted 28 August 2025
Available online 2 September 2025

data confidentiality and integrity, making blockchain particularly suitable for securing data flows within IoT ecosystems [15–17]. In some architectures, data distribution and processing are designed symmetrically to balance workloads across IoT nodes. This approach improves both efficiency and fault tolerance. The integration of blockchain in IoT offers improved data traceability, resistance to tampering, and trustless collaboration across devices, ultimately contributing to more dependable and scalable IoT infrastructures. For the context of this study, reliability is a system or component's ability to perform as needed in established conditions over a specified time without failure. Dependability, on the other hand, is a broader term that includes not only reliability but also availability, safety, integrity, and maintainability.

Given the potential of blockchain to enhance IoT security, interoperability, and trustworthiness, this paper conducts a systematic review of blockchain-based IoT integration. This analysis examines several approaches to integrating blockchain with IoT, which have a variety of applications. According to the observations from the background of current knowledge, the integration processes included in this study are categorized widely. The primary contributions of this work are as follows:

- Assessing and analyzing existing research studies on the integration of blockchain and IoT to identify different approaches.
- Identifying research gaps in blockchain-based IoT applications.
- Reporting trends and evolutions in the adoption of blockchain for IoT beyond cryptocurrency applications.

The contribution and motivation are presented in Section 2, and the research methodology is shown in Section 3. In Section 4, a suggested literature review for this paper is presented. Section 5 reports findings and discussions, while Section 6 evaluates obstacles and further work. Lastly, the conclusions and limits are stated in Section 7.

2. Contribution and motivation

The main aim of this research is to explore how blockchain and IoT can integrate to enhance reliability and dependability, identify new opportunities and challenges, and provide a systematic overview to guide future solutions in blockchain-IoT systems.

To complete this research study, existing investigations have been reviewed, including those previously published on this subject (such as studies on topics like surveys, bibliometrics, systematic reviews, future directions, and challenges related to blockchain technology and IoT). Fig. 1 shows the number of review publications by year of publication, which indicates the trend of growth or decline in scientific journals each year. As shown, the number of published articles has increased from 2016 to 2021, indicating a significant growth in research activities in this field. The decline in the publication rate of review papers during 2022 is likely to be a result of increased attention towards novel technologies or budget and economic challenges in academic research. A summary of the main objectives of ten systematic review studies is presented as an example.

A total of 205 relevant reviews concerning blockchain applications for the IoT were identified. We performed a search on Google Scholar utilizing the query: ("Blockchain" AND ("Internet of Things" OR "IoT") AND ("survey" OR "review" OR "state of the art")). Below, we summarize the primary contributions of ten systematic reviews that are related to this topic.

For instance, Conoscenti, Vetro [18] conducted a systematic review of current blockchain applications with special focus on conceptual needs such as anonymity (which they correctly called pseudonymity), integrity, and flexibility. They noted that while the PoW consensus algorithm ensures the integrity of data, its computational requirement makes adaptability in dynamic and resource-limited environments such as IoT a problem. This security-operational efficiency compromise has been a recurring theme in subsequent research.

Building on this, Lo, Liu [19] went further with an applied solution direction for the topic, concentrating on blockchain solutions to data and product management in IoT. While advocating stronger and improved evaluation techniques, their work is likewise limited largely to high-level architectural specification and does not examine mechanisms for resource allocation or optimization.

On the contrary, Tran, Babar [20] proposed a multi-dimensional taxonomy for the categorization of blockchain–IoT systems. They not only assessed technical integration but found ten varying archetypes of blockchain–IoT implementation, offering valuable information on prevailing convergence patterns. However, their focus was merely on system taxonomy and not on performance evaluation under actual-world constraints or low-resource settings.

Some studies, such as those by Hussain, Javed [21] in supply chain environments and Stefanescu, Montalvillo [22] with regard to lightweight blockchain platforms, have attempted to address performance concerns. Stefanescu's study is especially interested in reducing computational and memory overhead—a notably pertinent consideration in IoT environments. Yet such studies have not delved very far into adaptive, Artificial Intelligence (AI)-based mechanisms for dynamic resource allocation.

On the security front, Akinbi, MacDermott [23] researched the use of blockchain for IoT forensic analysis with the focus on its ability to upgrade the authenticity of legal proceedings. This application in a specific field reflects the strength of blockchain in critical environments, but performance at runtime, scalability, and resource consumption are not

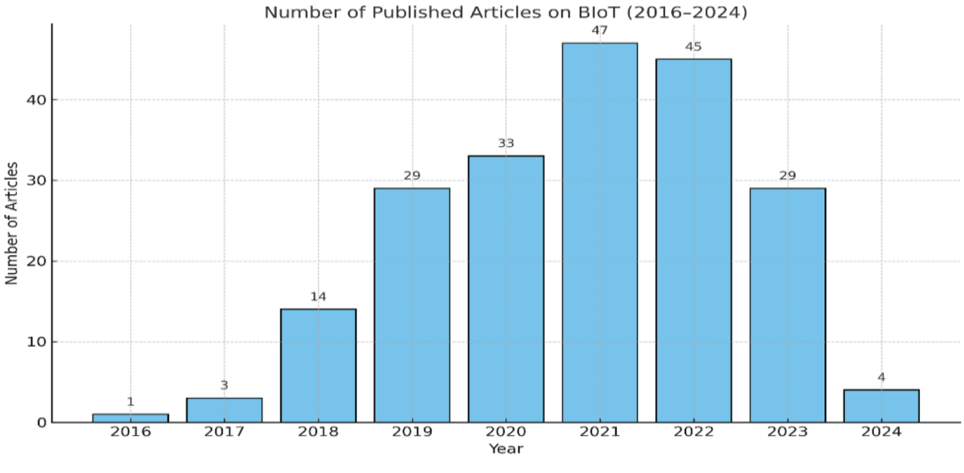

Fig. 1. Distribution of BIoT review articles from 2016 to 2024.

extensively explored.

In practical application examples, literature such as Adere [24] and Ahmed [25] presented blockchain applications in fields such as digital health, learning, and smart cities. These do mention privacy protection and access control, but are not serious technical assessments of the integration's limitations, such as latency or adaptive resource allocation.

In terms of governance and policy, Ivić, Milićević [26] and Alkhateeb, Catal [27] investigated blockchain's use in e-government service delivery and hybrid blockchain systems, respectively. While Ivić, Milićević [26] highlighted the requirement for non-technical factors such as legal frameworks and public trust, Alkhateeb, Catal [27] indirectly contributed towards the topic of resource-constrained environments by investigating complementary technologies, including edge and fog computing. However, the two studies all share the drawback of insufficient and limited evaluation of system performance within these environments. Table 1 presents a comprehensive classification and comparison of the relevant literature, emphasizing the focus and contributions of this paper.

Examination of each review article shows that the classification presented here is unique and approaches the literature from a different perspective. This review focuses on research articles published from 2020 onwards, offering the most up-to-date insights and a clear view of recent developments in the field.

3. Research methodology

This Systematic Literature Review (SLR) followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines [28] and was designed to provide a rigorous, repeatable process for identifying, evaluating, and synthesizing relevant research on the integration of Blockchain and the IoT (BIoT). The process included the development of research questions, selection of data sources, formulation of search strategies, application of inclusion and exclusion criteria, quality assessment, data extraction, and synthesis.

3.1. Research questions

The objective of this study was to investigate the convergence of blockchain and IoT technologies with a focus on reliability, security, and trust management. In order to gather pertinent material from a variety of sources, concentrating on the study objectives outlined in the questions in Table 2, a systematic review was performed. The following four research questions were developed in order to meet the study objective:

Table 2
Research questions.

#	Research Questions	Discussion
1	Why does the IoT employ blockchain technology?	The answer to this question is given in Section 4.
2	In what ways can blockchain address the security and trust management challenges of IoT, and what strategies and issues arise during the integration of IoT and blockchain?	The answer to this question is given in Section 4.
3	What are the existing mechanisms in the literature for IoT-enabled networks?	The answer to this question is given in Section 4.
4	What are the challenges and issues in blockchain-enabled IoT networks?	The answer to this question is provided in Sections 6 and 7.

3.2. Literature search and selection

We identified and selected studies for this SLR in a four-step process, as depicted in Fig. 2. The process of establishing information sources was the first stage in an SLR. To ensure comprehensive coverage of the literature, the Google Scholar, WoS, IEEE Xplore, and ACM digital databases were searched for papers for this SLR. These databases were widely recognized as leading sources for high-quality publications in computing and information technology. In order to locate papers pertinent to our subject, the next step was to define strategies for mining the scientific and technical materials that these searches had brought up.

Initial scoping reviews and previous surveys in the field of BIoT revealed a high degree of variation in terminology, approaches, and application contexts in research looking into reliability and dependability enhancement in BIoT systems. We initiated our study with a pilot search, combining the primary keywords blockchain and IoT and testing them individually. Based on the preliminary results, we identified relevant correlates and synonyms, allowing us to refine and expand our search string as shown below:

The following search string was applied across all databases:

"“blockchain-enabled Internet of Things” OR “blockchain-enabled IoT” OR BIoT OR “blockchain AND IoT”AND “fault-tolerant OR data integrity OR consensus mechanisms”".

Based on the specified search terms, as of July 1, 2024, the number of retrieved publications was as follows: 906 in Google Scholar, 450 in the WoS, 395 in IEEE Xplore, and 678 in the ACM Digital Library.

It was impractical to read so many articles from so many databases. Accordingly, to undertake an up-to-date systematic review, we employed a time restriction, e.g., studies within the period from 2020 onwards. That way, we ensured our systematic review embraces the most up-to-date and relevant studies. Following this filter, 312 records from the WoS database, 546 records from the Google Scholar database,

Table 1
Summarization of the reviewed papers.

Author(s)	Publication date	Database searched	Number of articles reviewed	Citations until Sep 2024
Conoscenti, Vetro [18]	August 01, 2016	IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, Google Scholar	35	955
Lo, Liu [19]	3 May 2019	Web of Science (WoS), Scopus, IEEE Xplore, ACM Digital Library	35	163
Tran, Babar [20]	23 July 2020	Scopus, IEEE Xplore, ACM Digital Library	120	33
Hussain, Javed [21]	10 December 2021	IEEEXplore, ACM Digital Library, ScienceDirect, Springer Link, Wiley Online Library, Sage Journals, Taylor & Francis Online, Google Scholar	44	85
Stefanescu, Montalvillo [22]	23 November 2022	dblp, Google Scholar, WoS, Scopus, IEEE Xplore, ACM	98	17
Akinbi, MacDermott [23]	1 October 2022	IEEE Xplore, ScienceDirect, ACM Digital Library, Springer Link	16	24
Adere [24]	12 March 2022	AIS, ACM Digital Library, IEEE Xplore, ICIS, INFORM	73	93
Ahmed [25]	6 November 2022	IEEE Xplore, Springer, ScienceDirect, WoS	50	3
Ivić, Milićević [26]	1 August 2025	Scopus	23	14
Alkhateeb, Catal [27]	9 February 2022	ScienceDirect, ACM Digital, IEEE Xplore, Wiley	38	67

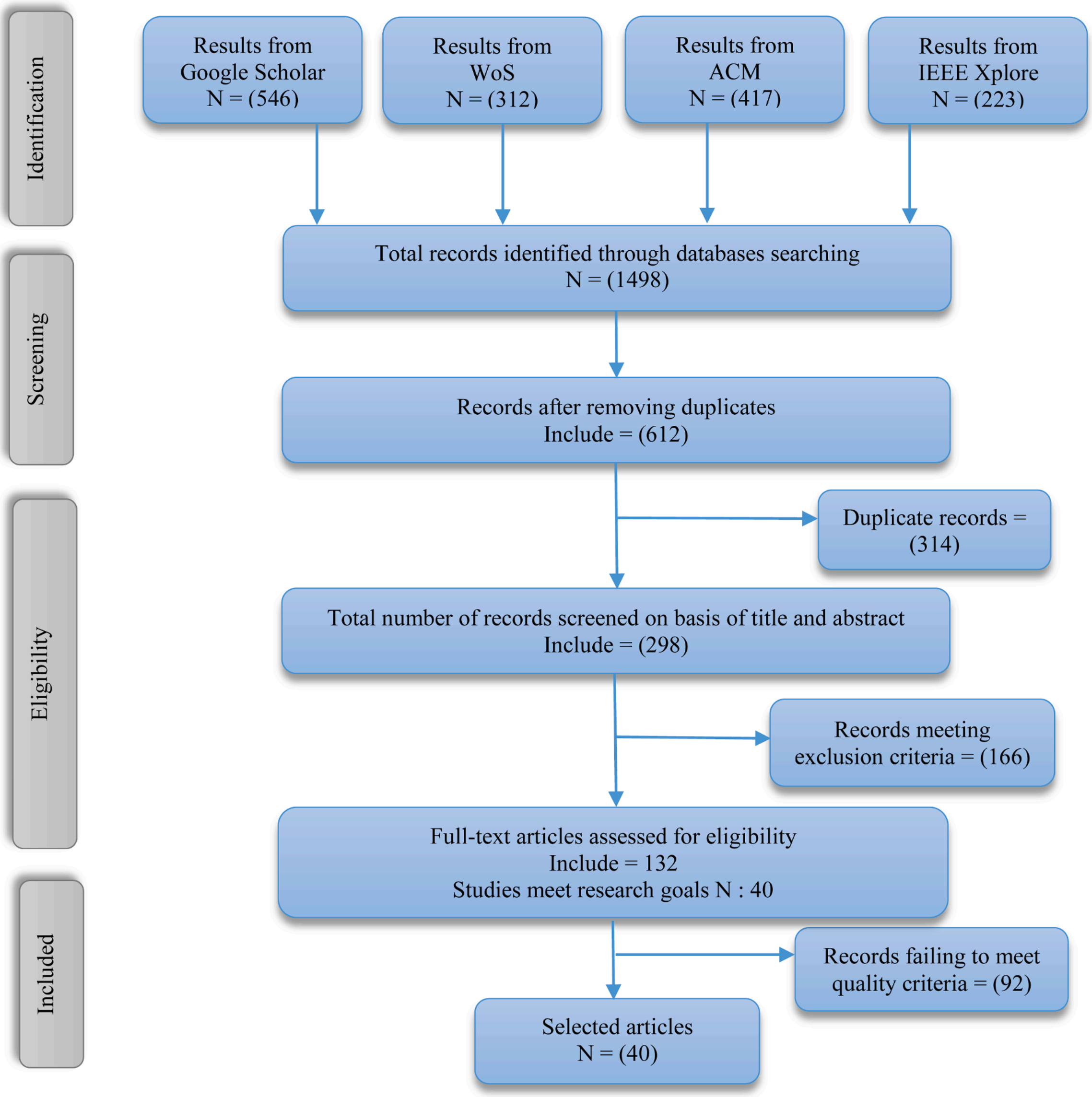
Identification
Screening
Eligibility
Included
Results from Google Scholar N = (546)
Results from WoS N = (312)
Results from ACM N = (417)
Results from IEEE Xplore N = (223)
Total records identified through databases searching N = (1498)
Records after removing duplicates Include = (612)
Duplicate records = (314)
Total number of records screened on basis of title and abstract Include = (298)
Records meeting exclusion criteria = (166)
Full-text articles assessed for eligibility Include = 132 Studies meet research goals N : 40
Records failing to meet quality criteria = (92)
Selected articles N = (40)

Fig. 2. Flow chart based on the PRISMA protocol.

417 records from ACM, and 223 records from IEEE Xplore were obtained. Subsequently, 886 duplicate articles were removed due to overlaps across databases. Of the remaining 612 articles, following the reading of article titles, removing irrelevant articles, review articles, and the book chapters from the list, 132 articles remained. During full-text screening, 92 articles were excluded for being out of scope. Finally, after reading the remaining articles according to the quality assessment, 40 articles were selected for systematic review.

3.3. Inclusion and exclusion criteria

Based on the study questions, we used some inclusion and exclusion criteria (see Table 3) to test the technical and topic validity of the selected studies. We only considered peer-reviewed journals or top-tier conference publications in the English language from January 2020 onwards. Grey literature, white papers, review-only articles, and articles focused entirely on cryptocurrencies or blockchain for financial systems were not considered.

Table 3
Included and excluded criteria.

#	Inclusion Criteria	Exclusion Criteria
1	The paper must be written in the English language	Not available as full-text
2	The selected paper must be relevant to blockchain technology and IoT	Grey literature (white papers, editorial comments, book reviews, government documents, and blog posts)
3	The article must have been published in a reputable journal or conference	Articles that provide a review of the literature
4	The article should be from 2020	Duplicate studies
5		

3.4. Bias assessment

In this step, a multi-stage screening process was conducted to remove duplicates, irrelevant studies, and non-primary research articles. In order to minimize subjective bias in the selection of studies, title/abstract screening and full-text eligibility were screened independently by two reviewers against the pre-established protocol. The reliability between the two reviewers was calculated using Cohen's Kappa coefficient, which revealed substantial reliability (κ = 0.79 for title/abstract screening and κ = 0.75 for full-text screening). All the discrepancies were discussed and resolved by consensus, and a third reviewer acted as an arbitrator where necessary. This provided rigor and consistency in the included studies.

3.5. Quality assessment

To ensure methodological rigor, we employed a domain-specific scoring rubric adapted to BIoT and engineering studies. The rubric consisted of five dimensions rated from 0 (absent) to 4 (excellent), with a total of 20 points achievable. Articles with ≥14/20 were retained for synthesis. The five criteria are presented in Table 4.

The quality evaluation outcomes (Table 11) show that most of the analyzed papers realized good to high methodological rigor. In particular, 45 % of the articles scored excellent (≥18/20), demonstrating solid contributions in architectural novelty, stringent consensus mechanisms, thorough performance evaluation, and reproducibility. Another 47.5 % of the research works ranked in the moderate category (15–17/20), showing acceptable but less thorough methodological depth, typically due to limitations in either quantitative performance reporting or experimental validation. Lastly, 7.5 % of the papers were rated as borderline (14/20), mainly because of innovation weakness or missing descriptions of consensus/fault-tolerance mechanisms.

4. Literature review

Real-time trustful data transfer is enabled by interconnected IoT devices in a blockchain network, eliminating the need for a central intermediary. Cyber-attack protection is essential for distributed systems that gather, analyze, and share large volumes of privacy-sensitive user data. In addition to network (Transport Layer Security (TLS)/SSL) or application layer (payload encryption), standard protocols now utilized in the IoT can safeguard user data with login and password authentication. Nevertheless, this security comes with substantial use of energy and hefty network overhead expenses. Blockchain's underlying cryptographic technologies offer reliable distributed authentication and permission for users and devices alike [30].

To categorize the literature in an organized manner, we categorized the selected publications into five main groups based on their intrinsic technological strategy and the specific approaches they apply to enhance reliability and dependability in blockchain-enabled IoT systems.

4.1. Consensus mechanisms

Consensus mechanisms are the cornerstone of blockchain networks, ensuring their integrity, reliability, and decentralization [31]. Blockchain consensus mechanisms are protocols distributed networks use to validate transactions and ensure trust [32,33]. Examples of these mechanisms include PoW, Proof of Stake (PoS), Delegated PoS (DPoS), PBFT, Proof of Space-Time (PoST), Proof of Authority (PoA), etc [34].

Table 4
Quality checklist [29].

Item	Assessment Criteria	Score	Description
1	Architectural novelty	0–4	Originality and contribution of the proposed BIoT architecture or design
2	Consensus/fault tolerance/ integrity mechanisms	0–4	Use of blockchain consensus and resilience strategies
3	Quantitative performance criteria	0–4	Latency, throughput, scalability, energy consumption, etc.
4	Experimental validation	0–4	Validation via simulation, testbed, or real deployment
5	Clarity and reproducibility	0–4	Transparency of methodology, data, and replicability

4.1.1. Introduction to consensus mechanisms

Consensus algorithms are the foundation of blockchain networks, with their selection specifying how nodes come to agree on transaction validity and the shared state of the ledger. In IoT systems utilizing blockchain in areas such as resource-constrained deployments, the selection of a consensus protocol has a direct influence on energy efficiency, latency, scalability, and fault tolerance. Recent research has looked at lightweight and application-specific designs for consensus to address the specific requirements of IoT applications, trading off security guarantees against operational efficiency. In the following section, we review notable research works that have implemented various consensus mechanisms in blockchain-IoT systems.

4.1.2. Overview of selected consensus-based mechanisms

Misra, Mukherjee [35] introduced a lightweight blockchain framework for resource-constrained IoT edge networks. The system utilized a private Ethereum blockchain with the Clique – PoA consensus to reduce energy and latency overhead. A key contribution was the use of a centralized, encrypted time server, enabling secure synchronization across IoT devices lacking real-time clocks. Although no explicit fault-tolerant scheme was used, the design ensures secure data exchange and scalability.

Alrubei, Ball [36] proposed a secure blockchain platform integrating AI, IoT, and edge computing to support real-time data processing and sharing. It used a novel consensus mechanism called Honesty-based Distributed PoA (HDPoA) for fault tolerance and data integrity. The system was experimentally validated for COVID-19 detection with high accuracy and low energy consumption on low-cost devices.

Chen, Lin [37] developed BCC-SEL, a secure edge learning framework tailored for industrial IoT environments. It combined LaGrange coded computing to leverage idle edge nodes and tolerate stragglers, a blockchain with PoS consensus and smart contracts as an incentive and role-assignment mechanism, and a cosine-similarity validation step to detect and penalize malicious participants. The framework thereby addressed resource efficiency, motivation of honest nodes, and robustness in adversarial scenarios.

Qiu, Wang [38] introduced a blockchain-assisted collective Q-learning framework for resource allocation in cloud–edge–end IoT networks. It proposed proof-of-learning, a novel consensus mechanism replacing traditional PoW, enabling decentralized training and verifiable model sharing among lightweight IoT nodes, while improving learning efficiency and trust.

Hosen, Sharma [39] presented SECBlock-industrial IoT, an edge-computing framework for industrial IoT that integrates a consortium blockchain with InterPlanetary File System (IPFS)-based immutable storage and a hybrid cryptographic scheme (elliptic curve cryptography, physical unclonable function, LaGrange interpolation) to secure P2P and group communications. A modified PoV consensus algorithm reduced latency and failure risks in block mining. A deep learning-based threat detection model (autoencode + Recurrent Neural Network (RNN)- deep learning) identified cyber-attacks, offering improved efficiency and scalability.

Alrubei, Ball [40] also proposed a decentralized architecture for implementing distributed AI over IoT systems. Each IoT device functions as a neuron, and secure communication was enabled through a custom blockchain platform. A hybrid consensus mechanism called HDPoA (combining lightweight PoW and PoA) was introduced to ensure trust, efficiency, and scalability in non-financial IoT environments. Experiments demonstrated high accuracy (92–98 %) and low energy consumption, validating the feasibility of the approach.

Kumar, Harjula [41] designed BlockEdge, a blockchain-edge framework for industrial IoT that leverages lightweight permissioned blockchains at the edge for secure, low-latency operations and fog-level public blockchains for inter-organization trust. Simulations showed improved latency, energy efficiency, and network usage compared to non-blockchain setups.

The paper by Lin, Wu [42] introduced a blockchain-based framework for secure energy and knowledge trading in IoT systems. It integrated BFT-DPoS consensus, federated edge learning, and wireless power transfer, using a game-theoretic model to optimize incentives and energy usage. The system ensured secure data exchange, decentralized learning, and efficient power management.

Sarhan, Lo [43] proposed hierarchical blockchain-based federated learning, a hierarchical blockchain-based federated learning framework for secure, privacy-preserving IoT intrusion detection. Using smart contracts on a permissioned blockchain, enabled a collaborative model training across organizations without sharing raw data. Hierarchical blockchain-based federated learning improved detection accuracy and defended against attacks, validated through experiments on IoT data.

Finally, Mhaisen, Fetais [44] developed a cost-efficient IoT monitoring framework using smart contracts on the Ethereum blockchain. It employed deep reinforcement learning to optimize sensor data submission rates, balancing security (auditability and automation) with transaction costs: the solution leveraged blockchain consensus, decentralized oracles for fault tolerance, and immutable ledgers for data integrity.

4.1.3. Comparative analysis of reviewed consensus-based mechanisms

Table 5 below compares the reviewed consensus-based approaches in terms of platform, issues addressed, evaluation methods, efficiency, scalability, and cost.

As seen in the table, each consensus method involves trade-offs between performance metrics, making them suitable for different IoT scenarios. Integration of blockchain in IoT systems enhances security, integrity, scalability, and efficiency, with design-variable trade-offs. Public blockchains like Ethereum ensure strong security at the cost of high transaction fees and computation overhead, while permissioned and consortium models are less expensive and more scalable for industrial use cases. Lightweight or hybrid consensus protocols (e.g., PoA, HDPoA, BFT) and pairing with AI, federated learning, and IPFS also reduce latency, optimize resources, and improve anomaly detection capabilities. Together, findings cite up to 40 % CPU overhead in public chains, transaction cost from $1.80 to $0.05, 15–30 % improvement in efficiency, and scalability from hundreds to over 50,000 devices.

4.2. Fault-Tolerant designs

Distributed IoT environments inherently face a spectrum of faults—from device failures to adversarial threats—necessitating robust fault-tolerant design strategies. These architectures employ hierarchical consensus protocols, hybrid consensus models tailored for resource-constrained networks, and scalable clustering approaches to sustain reliability under real-world conditions [45,46].

4.2.1. Introduction to fault-tolerant designs

Ensuring uninterrupted and dependable operation in blockchain-enabled IoT requires fault-tolerant designs that can withstand node failures, network instability, and cyber threats. We now highlight selected studies that address fault tolerance in blockchain-enabled IoT networks.

4.2.2. Overview of selected fault-tolerant -based designs

For instance, Garlapati [47] categorized architectures into

Table 5
Comparison analysis of reviewed consensus-based mechanisms for blockchain-enabled IoT.

Ref.	Blockchain Platform	Issues Addressed	Method of Investigating	Efficiency Improvement	Scalability	Cost
[35]	Ethereum blockchain	Addressing IoT edge device limitations causing insecure data and vulnerability to unauthorized access.	Encrypted network-based time-synchronization mechanism	High security, but 40 % higher computational load on IoT nodes.	500 devices, 10–15 TPS	$0.50–$1.80 per transaction (high gas fees)
[36]	Public blockchain	Addressing security issues	AI	$0.40–$1.50 per transaction, $60,000 infrastructure cost	5000–8000 devices, 50–200 TPS	AI-driven real-time security, 10 % faster anomaly detection
[37]	Custom Blockchain-based Platform	Addressing privacy concerns and data integrity issues in edge learning environments	Simulation and experimental evaluation	Around 15–25 % improvement in learning accuracy and latency reduction	Designed for industrial IoT scale; supports multiple edge nodes	Medium
[38]	Any	Addressing issues such as the need for high processing power, inefficient training, and centralized training	Q-learning	$20,000 setup, $0.15 per transaction	10,000 devices, 150–300 TPS	20 % reduction in computational overhead using collective Q-learning.
[39]	Consortium blockchain + IPFS	Addressing key concerns in edge-IoT environments, including security, latency, and real-time threat detection capabilities	Modified PoV + deep learning -based ITD	Lower latency, higher detection accuracy	Supports large industrial IoT networks	Low
[40]	Public blockchains	Implementation of AI into the IoT	Distributed AI	25 % reduction in resource consumption	5000 IoT devices	High
[41]	Private/ permissioned blockchain and Public blockchain	Examining industrial process needs for performance, efficiency, and security.	Conceptual blockchain-edge-based framework	30 % improvement in process monitoring, secure industrial IoT transactions.	50,000+ devices, 500–1000 TPS	$100,000 initial deployment, $0.20 per transaction
[42]	Permissioned blockchain	Investigating the dilemma between limited battery capacity in the device and high energy demand in learning	Wirelessly powered edge intelligence	$75,000 deployment cost, $0.05 per transaction	20,000+ devices, 200–800 TPS	15 % increase in energy efficiency, Stackelberg-game model optimizations.
[43]	Permissioned blockchains	Providing a secure design, deploying a scalable IoT ecosystem, and ensuring data privacy	FL	20 % False Positive Reduction	Multi-Organization (Cloud-Fog-Edge)	Medium
[44]	Ethereum public blockchain	Examining the challenges associated with implementing blockchain-based IoT monitoring systems	Reinforcement learning	33 % reduction in transaction costs	500 devices (Ethereum simulation)	Low

LiTiChain, p-LiTiChain, and s-LiTiChain. Fault tolerance was handled via limited block lifespan, lightweight blocks, and block subdivision, respectively. Data integrity relies on block retention and packaging strategies. These mechanisms improve scalability and security in IoT blockchains.

Jamil, Kahng [48] proposed a secure fitness monitoring framework using IoT devices integrated with blockchain (Hyperledger Fabric) and machine learning algorithms. It ensured data integrity through encryption and smart contracts, while consensus is achieved via Fabric's endorsement and ordering services. Fault tolerance was addressed through peer replication.

Latif, Wen [49] introduced a security architecture integrating AI, blockchain, and Software Defined Networking (SDN) to protect IoT-based cyber-physical systems. It used blockchain for decentralized consensus, SDN for centralized control and traffic monitoring, and AI models for anomaly detection. Fault tolerance was supported through distributed ledger replication and resilient network routing, while data integrity was ensured using blockchain immutability and secure communication protocols.

Cai, Liang [50] presented blockchain-Directed Acyclic Graph (DAG)-based consensus for fast, scalable validation. It used a distributed prophecy machine for off-chain data and IPFS for secure storage. Fault tolerance relied on the DAG structure and distributed data retrieval, while data integrity was ensured via SHA-256 hashing and zero-knowledge proofs.

Wu, Liao [51] developed a decentralized and secure IoT framework using BFT as its consensus mechanism within a permissioned blockchain architecture. The system ensured trust and security at the network edge by leveraging fault-tolerant design principles and distributed ledger technology. It protected data integrity through cryptographic hashes and access control, aiming to balance performance, scalability, and trust in resource-constrained IoT environments.

4.2.3. Comparative analysis of reviewed fault-tolerant-based designs

Table 6 summarizes the main characteristics and performance outcomes of the reviewed fault-tolerant designs.

The table illustrates how fault-tolerant architectures differ in complexity, scalability, and cost-effectiveness. LiTiChain [47] minimizes latency and energy consumption for edge-IoT, whereas Hyperledger Fabric [48,51] enhances privacy, accountability, and resilience using endorsement-ordering and BFT-based edge infrastructures. Large-scale architectures [49] attain 40 % less energy consumption for 100,000 devices, whereas DAG-based frameworks [50] attain improved security for IoT with 10.5 % quicker processing. Throughput, efficiency, and availability are generally improved, but the trade-offs depend on application scope, scalability, and fault-tolerant requirements.

4.3. Data integrity techniques

Data integrity is foundational in blockchain-enabled IoT systems, ensuring that IoT-generated data remains accurate, consistent, and tamper-resistant throughout its lifecycle. Blockchain's cryptographic primitives—such as hashing and digital signatures—combined with decentralized ledger architectures, provide immutable and verifiable records, making data manipulation computationally infeasible [52,53].

4.3.1. Introduction to data integrity techniques

Integrating blockchain within wireless sensor networks has demonstrated robust performance in preserving data authenticity, traceability, and scalability, particularly in environments prone to cyber-attacks and untrusted devices [54]. Below, we examine key studies focusing on data integrity approaches in blockchain-enabled IoT systems.

4.3.2. Overview of selected data integrity-based techniques

For example, Shahbazi and Byun [55] proposed a blockchain-based smart manufacturing system leveraging Hyperledger Fabric, integrating IoT sensors and machine learning for real-time quality control and security enhancement. The consensus mechanism relied on endorsement and ordering services native to Hyperledger Fabric. Fault tolerance was managed through a permissioned blockchain structure with distinct roles (endorsers and committers). Data integrity was ensured via digital signatures, smart contracts, and digital identities, controlling data access and privacy.

Khan, Byun [56] developed an IoT-blockchain system for food supply chains using Hyperledger Fabric's consensus for secure transactions. Fault tolerance was supported by blockchain decentralization and endpoint security. Data integrity was ensured via cryptographic hashes and smart contracts. Advanced deep learning with Genetic algorithm optimization enhances supply chain transparency and prediction.

Saravanan, Madiajagan [57] proposed a secure intrusion detection framework integrating blockchain, identity-based encryption, and an optimized RNN using African buffalo optimization. The blockchain ensured data immutability and secure sharing in cloud environments, while the African buffalo optimization-enhanced RNN improves detection accuracy and speed. The approach achieved high performance, with an accuracy of 99.87 % and a recall of 99.92 %.

Table 6

Comparison of fault-tolerant designs for blockchain-enabled IoT.

Ref.	Blockchain Platform	Issues Addressed	Method of Investigating	Efficiency Improvement	Scalability	Cost
[47]	LiTiChain	Addressing critical constraints in edge-IoT, including storage overhead, data freshness, latency, and limited energy resources.	Analytical modeling and simulations	Reduced latency, improved data freshness, and optimized energy consumption	Moderate – suited for limited-lifetime data	Low
[48]	Hyperledger Caliper	Providing a new approach to guarantee data accountability, enhance data privacy and accessibility, and uncover latent patterns and valuable insights to deliver sufficient services	decision tree, logistic regression, SVM, and K-nearest neighbors	15 % throughput increase	2000 users	Medium
[49]	Private and public blockchain	Concentrating on reducing a few of the obstacles associated with the IoT	AI	40 % reduction in energy consumption	100,000 units	Very high
[50]	Any	Addressing IoT security risks and their susceptibility to attacks	Graph neural networks	10.51 % processing speed improvement	1000 nodes	Low
[51]	Permissioned Blockchain (Hyperledger Fabric-based)	Addressing challenges related to data privacy and ownership, single points of failure, data trust and integrity, and tolerance to Byzantine faults in edge-IoT environments	Prototype implementation of Reja framework, latency and throughput testing of Reja and ChiosEdge modules	Lower latency due to edge computing integration, fault-tolerant data replication	Edge-based deployment supports distributed scaling, consensus optimized for edge devices	Implementation cost not explicitly quantified

Otoum, Al Ridhawi [58] introduced a decentralized framework that integrates federated learning with blockchain and reinforcement learning to enhance trust and security in critical IoT infrastructures. The system enabled local model training with privacy, verified updates using blockchain, and achieved high accuracy (~0.93) and detection rates (~0.96) while reducing energy use and extending network lifetime.

Ratnayake, Liyanage [59] by Ratnayake et al. proposed a blockchain-based IoT data trust system using machine learning. It combined Support Vector Machines (SVM) on edge servers and ensemble machine learning models (multilayer perceptron, k-nearest neighbors, random forest) on validators to assess data trust. Raft consensus ensured agreement, IPFS handles off-chain storage, and smart contracts manage validation and reputation. This design improved trust accuracy and data integrity in decentralized IoT networks.

Ali, Almaiah [60] presented a secure Industrial IoT healthcare framework using Hyperledger Fabric for consensus, ensuring reliable data sharing via blockchain and trust chain for fault tolerance. Data integrity was maintained through homomorphic encryption and searchable encryption, enabling secure and private access to patient records.

Sizan, Dey [61] proposed an IoT- machine learning-blockchain framework for crop prediction, focusing on data integrity through cryptographic hashing and immutable ledgers. It did not specify consensus mechanisms or fault-tolerant designs, emphasizing secure and transparent data management in smart agriculture.

He, Wang [62] proposed a blockchain-enabled framework for allocating edge computing resources in IoT scenarios using deep reinforcement learning. It integrated A3C (Asynchronous Advantage Actor–Critic) within smart contracts to dynamically assign edge computing nodes based on users' quality of service needs. Blockchain supported trustless coordination and immutable transaction logging, while the A3C agent optimizes resource allocation to balance latency and efficiency.

Kumar, Kumar [63] developed a blockchain-based IoT healthcare framework using PoA consensus for efficient validation. It incorporated partial fault tolerance through distributed validation and layered architecture. Data integrity was ensured by zero-knowledge Proofs, blockchain immutability, IPFS storage, and smart contracts to protect healthcare data.

4.3.3. Comparative analysis of reviewed data integrity-based techniques

Table 7 presents the comparative assessment of these techniques regarding their platform, methods, efficiency, scalability, and cost.

The comparison highlights that strong integrity measures often come with computational and cost trade-offs. Hyperledger Fabric and permissioned blockchains, in combination with ML algorithms (e.g., XGBoost, RNN, SVM), achieve 27–40 % performance improvement in error detection and authentication efficiency. Public blockchains and federated learning improve anomaly detection and consensus accuracy by up to 25 %, at the expense of higher computation. Integration with IPFS, cryptographic hashing, and smart contracts ensures secure, scalable, and tamper-proof data management. Overall, blockchain choice should balance security, efficiency, and scalability according to application requirements.

4.4. Lightweight blockchain-based mechanisms

Since IoT devices have a resource-constrained environment, this category prioritizes research that recommends efficient blockchain structures, such as lightweight consensus mechanisms and reduced computational overheads, to ensure efficacy without any sacrifice in security and trust.

4.4.1. Introduction to lightweight blockchain-based mechanisms

When examining lightweight blockchain solutions, the predominant focus among researchers is the computational overhead associated with blockchain utilization. While blockchain delivers essential security and privacy enhancements to networks comprising untrusted devices, these benefits often incur significant computational costs. A primary area identified by many scholars as contributing to the computational burden of blockchain is its consensus algorithm, prompting the exploration of numerous alternatives to the traditional PoW consensus algorithm [22]. This investigation reveals a diverse array of approaches for implementing blockchain networks, underscoring the evident gap in the availability of a streamlined, universally accepted, and standardized testing and evaluation platform tailored for lightweight blockchain systems. The following reviewed works illustrate how lightweight approaches balance efficiency and security in blockchain-IoT integration.

4.4.2. Overview of selected data integrity-based techniques

For instance, Alkhazaali and Oğuz [64] proposed a lightweight blockchain-fog architecture for IoT, using RAFT consensus and TLS to ensure privacy, low latency, and efficient resource use. The system distributes processing across fog nodes and utilizes virtualization

Table 7
Comparison of Data Integrity Techniques for Blockchain-enabled IoT.

Ref.	Blockchain Platform	Issues Addressed	Method of Investigating	Efficiency Improvement	Scalability	Cost
[55]	Private Hyperledger Fabric	Predicting the reliability and quality of equipment and industrial data security and management	XGBoost algorithm	27 % Error Detection	50,000 transactions/day	High
[56]	Private Hyperledger Fabric	Having serious concerns about food safety and transparency in the food supply chain	RNNs	40 % reduction in authentication time	1000+ concurrent users	Medium
[57]	Any	Investigation of malicious attacks and intrusions (attacks)	RNN	12 % Accuracy Improvement (F1-Score)	50,000 transactions/day	Medium
[58]	Public blockchains	Safeguarding sensitive data from modification and exploitation by unreliable parties, especially when it pertains to important applications	FL	18 % improvement in consensus accuracy	10,000 devices (MATLAB simulation)	Medium
[59]	Hyperledger Fabric v2.4	Addressing key challenges in edge-IoT environments, including privacy concerns, data integrity issues, storage overhead, data freshness, latency, and energy constraints	SVM, multilayer perceptron	~5–15 % improvement over baseline models (accuracy >90 %)	Uses IPFS for off-chain storage	Medium
[60]	Hyperledger Fabric	Examining challenges such as security, reliability, trustworthiness, confidentiality, etc	Hybrid deep neural network	35 % reduction in search time	1000 patients	High
[61]	Generic blockchain with smart contracts	Addressing challenges related to data distrust, insecure storage, and limited predictive insights in edge-IoT environments	SVM model	97.73 % SVM prediction accuracy	Moderate (7 sensors + cloud-based app)	Low to Moderate
[63]	Public Ethereum blockchain	Establishing a secure link between servers and IoT devices to fend off hackers who could attempt different cyberattacks that might put patients at danger of being seriously monitored	Deep learning approach	25 % increase in detection speed	5000 medical devices	Medium

(Docker) for scalability. Performance results showed low Central Processing Unit (CPU)/ Random Access Memory (RAM) usage and stable response times, making it suitable for resource-constrained IoT.

Guruprakash and Koppu [65] enhanced a lightweight scalable blockchain for IoT by using Elliptic curve ElGamal (EC-ElGamal) encryption to secure transactions and a Genetic algorithm to optimize SHA-384 hashing. These enhancements boosted security, fault tolerance, and data integrity while improving transaction and block validation performance in resource-constrained IoT networks.

Park and Park [66] introduced a two-class data transmission system using dual blockchains (lightweight and conventional) for smart dust IoT environments with minimal computing capacity. Urgent data was transmitted immediately using a simplified blockchain with SHA-256 hashing for integrity, while normal data undergoes a time-scheduled process via standby and main ledgers to reduce congestion. Although consensus mechanisms like mining were excluded, the system ensures data integrity and fault tolerance by leveraging unique transaction structures and dual ledger architecture.

Bandara, Tosh [67] presented Tikiri, a lightweight blockchain for IoT. The system used Kafka with federated voting for consensus, employs sharding and reactive streaming for fault tolerance, and ensured data integrity via digital signatures and off-chain proofs. These features target scalability and efficiency for resource-constrained IoT environments.

Qin, Huang [68] introduced LBAC, a lightweight access control model that integrates attribute-based encryption with Hyperledger Fabric blockchain to ensure secure data access in IoT. It performed outsourced decryption through smart contracts to reduce overhead on constrained devices, assumes an untrusted cloud, and introduced a credibility-based user incentive mechanism to adjust endorsement policies dynamically.

Li, Zhang [69] proposed a lightweight blockchain for IoT using an improved PBFT consensus with a reward-punishment strategy to lower communication costs. They also applied Reed-Solomon erasure coding for efficient, fault-tolerant storage. Results showed reduced delay and storage overhead, making it suitable for resource-constrained devices.

Said [70] proposed LBSS, a lightweight blockchain-based security scheme designed for IoT-enabled healthcare environments. The system used blockchain to ensure secure data transmission and decentralized trust. A lightweight consensus protocol was adopted to reduce computational overhead, making it suitable for resource-constrained medical IoT devices. The scheme ensured fault tolerance through distributed architecture and improved data integrity using cryptographic techniques and secure data logging.

LightCert4IoT, proposed by [71], is a lightweight blockchain-based certificate system designed for constrained IoT devices. It involves IoT devices, Local Registration Authorities (LRA), and the Ethereum blockchain. The system employs Ethereum's PoW consensus, LRAs for fault tolerance, and Merkle trees for ensuring data integrity. LightCert4IoT optimizes certificate size to enable secure and scalable device authentication.

Finally, Ullah, Oleshchuk [72] proposed a lightweight attribute-based access control scheme tailored for blockchain-enabled IoT. It enhanced access control flexibility by using attribute policies instead of centralized control, leveraging blockchain's decentralized ledger for secure, transparent management of access rights—the scheme employed hyperelliptic curve cryptography to achieve efficiency and security.

4.4.3. Comparative analysis of reviewed lightweight blockchain-based mechanisms

Table 8 compares lightweight blockchain-based mechanisms by platform, key issues, methods, efficiency, scalability, and cost.

Lightweight blockchain technologies for IoT improve efficiency, scalability, and security by minimizing computation, communication, and storage overhead. RAFT-based Hyperledger Fabric provides

Table 8
Comparison of lightweight blockchain-based mechanisms for blockchain-enabled IoT.

Ref.	Blockchain Platform	Issues Addressed	Method of Investigating	Efficiency Improvement	Scalability	Cost
[64]	Hyperledger Fabric	Addressing security and privacy concerns, latency issues, and resource limitations in IoT–fog environments	System design and performance evaluation with 1000 transactions	Reduced response time (<100 s) and RAM usage (<300 MiB)	High scalability due to RAFT consensus suitable for consortium blockchain	Low
[65]	Lightweight scalable blockchain	Improving lightweight scalable blockchain for better adoption in IoT	EC-ElGamal and Genetic algorithm-based key for SHA-384	42 %	Medium	Moderate
[66]	Two kinds of blockchains with two different ledgers	Exploring issues related to urgent data transfer and potential security challenges in deploying IoT systems in hard-to-access areas	An effective transmission method for two-class sensed data for secure smart IoT systems	53–96 %	High	Low
[67]	Tikiri blockchain	Addressing IoT-blockchain integration challenges like search, real-time response, performance, and throughput	Tikiri consensus using Apache Kafka	48 %	High	Low
[68]	Fabric blockchain	Investigating the limited resources of IoT devices to perform expensive operations	Lightweight decryption based on attribute-based encryption and blockchain	27 %	Medium	Moderate
[69]	Private blockchain	Exploring the limited resources of IoT devices to handle the demands of the blockchain consensus procedure	PBFT blockchain consensus mechanism based on reward and punishment strategy	44 %	High	Low
[70]	Any	Establishing a reliable and highly secure healthcare system	Lightweight Security Scheme	29 %	Medium	Moderate
[71]	Any	Examining the security issues of decentralized PKIs based on blockchain technologies	Alternative to the PKI model	47 %	Medium	Low
[72]	Lightweight Blockchain IoT	Addressing the need for secure decentralized access control while minimizing computation and communication overhead in IoT–fog environments	Comparative analysis and performance evaluation	Reduced computation & communication overhead compared to previous schemes	Supports scalable access control via attribute-based policies	Low computational cost

response time <100 s and RAM usage <300 MiB, whereas lightweight encryption and multi-ledger designs optimize transaction speed (up to 96 %) and throughput (up to 48 %). The designs preserve tamper-proof access control, secure logging, and fault tolerance, providing a resource-saving, scalable solution for industrial, healthcare, and edge-IoT scenarios.

4.5. *Multi-tier based mechanisms*

These mechanisms are hierarchical or tiered architectures with different tiers (e.g., cloud, edge, and IoT devices) working together to offload computational workloads and enhance the reliability of systems.

4.5.1. *Introduction to multi-tier based mechanisms*

Multi-layer-based mechanisms within blockchain-based IoT partition the work into different layers to enhance scalability as well as security. Sub-engines, in such cases, can be deployed locally near IoT devices to manage multiple nodes efficiently [73]. Selected studies below show how multi-tier designs enhance scalability and security in IoT-blockchain environments.

4.5.2. *Overview of selected multi-tier based mechanisms*

For example, Corradini, Nicolazzo [74] introduced a two-tier blockchain system for IoT trust management, using local ledgers for device reliability and a global ledger for cross-community reputation. It ensured secure, autonomous IoT interactions with lightweight consensus and distributed trust evaluation.

Mišić, Mišić [75] proposed a multi-tier blockchain architecture for IoT systems using a modified PBFT consensus with dynamic leader selection via bandwidth reservation. The model enhanced fault tolerance by reducing reliance on a fixed leader and improves data integrity through tiered block validation. An analytical model was used to minimize block linking time under geographic and load constraints.

Liu, Su [76] secured IoT task data using intelligent reflecting surface-based physical layer security and allocated edge computing resources with a Gas-driven offloading strategy. Their method reduced energy use and ensures fair resource access, outperforming existing schemes.

Dai and Xia [77] introduced GH-PBFT (grouped and layered consensus), which enhances PBFT by structuring nodes into hierarchical groups and performing layered consensus to reduce communication and latency. They employed fault-tolerant mechanisms through node grouping and the 2f+1 quorum rule, and utilized CLS to minimize certificate overhead, thereby improving data integrity and overall system efficiency.

Wang, Zhang [78] proposed a two-blockchain federated learning system with hierarchical clustering for industrial IoT data. It improved model accuracy, privacy, and efficiency by combining synchronous and asynchronous training and using encrypted model storage.

Bary, Elomda [79] presented a Multi-Layer Blockchain Security Model (MLBSM) to enhance privacy and scalability in IoT networks. It used a public Layer-1 blockchain for interoperability and transaction verification, and a private Layer-2 blockchain for localized data control. The model applies symmetric cryptography for secure communication and clusters IoT nodes to minimize privacy leakage and manage authentication without a centralized authority.

Xu, Yu [80] introduced MTEC, a multi-tier blockchain storage architecture using Reed-Solomon erasure coding to address IoT storage challenges. It reduced replication overhead, improved query efficiency through block pre-loading and node collaboration, and achieved high storage optimization while preserving data reliability.

4.5.3. *Comparative analysis of reviewed multi-tier-based mechanisms*

Table 9 summarizes multi-tier blockchain mechanisms, highlighting platforms, methods, efficiency, scalability, and cost. These approaches improve scalability and resource balance but add deployment complexity.

Recent research shows that multi-tier blockchain mechanisms for IoT are effectively dealing with security, scalability, energy consumption, and storage overhead issues. Two- and multi-tier architectures [74,75] have sustained thousands of devices with low latency and stable trust event registration, while PLS, GH-PBFT, multi-layer federation, and PoC based mechanisms [76–79] have reported significant gains in energy efficiency, federated learning model stability, and TPS throughput. Further, the application of Reed-Solomon erasure coding [80] considerably lowered storage overhead and cross-tier query costs.

Tables 5–9 overview the key performance characteristics of the surveyed BIoT solutions, according to different consensus mechanisms, deployment scenarios, and application domains. Performance metrics reported in the literature—namely, latency, throughput, energy consumption, and storage efficiency—demonstrate a wide range due to heterogeneity in experimental environments, network sizes, transaction

Table 9
Comparison of multi-tier blockchain-based mechanisms for blockchain-enabled IoT.

Ref.	Blockchain Platform	Issues Addressed	Method of Investigating	Efficiency Improvement	Scalability	Cost
[74]	Public blockchain	Addressing two significant obstacles: the requirement to ensure the autonomy of smart things and their protection	Two-tier blockchain framework	50–100 trust evaluations per community	Scalable to 500 nodes per tier	Approx. $5000-$10,000 for blockchain maintenance
[75]	Permissioned blockchain	Examining the security issues of consensus protocols that rely on a rotating leader	Multi-tier blockchain framework, PBFT consensus algorithm	Up to 1000 IoT devices, 5-tier setup	Supports 10,000 devices, latency <100ms	~$10,000 per node
[76]	Ethereum public blockchain	Exploring energy-efficient and physically secure computation offloading in blockchain-empowered IoT systems	Using PLS	20 % improvement in energy efficiency	Scalable to 500 IoT devices	~$12,000 for intelligent reflecting surface modules
[77]	Lightweight three-tier IoT	Addressing resource constraints and certificate management overhead in IoT and fog-based environments	GH-PBFT consensus + certificateless encryption	Reduced communication overhead	Hierarchical consensus groups	Lower resource usage
[78]	Blockchain Multi-layer Federation	Solving the problems of data heterogeneity and privacy protection in the industrial IoT	Multi-layer group federation scheme based on dual-blockchain	30 % improved convergence stability in federated learning	Supports up to 2000 devices	~$18,000 for federated learning setup
[79]	Lightweight blockchain	Addressing IoT security challenges, including privacy, authentication, adaptability, and scalability	Utilization and validation of the open-source HLF blockchain	1000–2000 TPS (lower tiers), 100 TPS (top tier)	Scalable to 10,000 devices	~$15,000 for clustering and energy efficiency
[80]	Multi-tier Blockchain	Addressing high storage overhead and cross-tier query costs in IoT–blockchain systems	Design and implementation of MTEC using Reed-Solomon erasure coding	86.3 % storage reduction; 15.8 % better than MLDC; 7.35 % lower query cost	Scalable across multi-tier architecture for IoT	Not explicitly reported

payloads, and evaluation methodologies.

In general, research works relying on lightweight or optimized BFT-type consensus protocols achieve significantly lower latency and higher throughput than conventional PoW systems. Multi-layered architectures combined with erasure coding were found to lower storage overhead by over 80 %, and specially optimized PBFT protocols for healthcare and industrial IoT use cases have exhibited up to 44 % latency benefits. Energy efficiency benefits were usually expressed as percentage improvement over a baseline; absolute figures in joules per transaction were comparatively rare, though, so quantitative summarization across studies was harder.

One of the prevailing limitations apparent in Tables 5–9 is the absence of consistent reporting of performance metrics. While some studies reported relative improvements with no descriptions of baseline conditions, others omitted critical experimental parameters such as node hardware specifications or transaction sizes. Cost metrics were also reported in heterogeneous formats (e.g., USD per transaction, gas units, or qualitative descriptions), further hindering direct comparability. These discrepancies highlight the urgent need for standardized benchmarking protocols to enable fair and reproducible cross-platform comparisons.

5. Results and discussions

The ongoing research delves into the prevailing challenges and complexities surrounding BIoT applications. In this regard, in the previous section, 40 articles were examined in detail in 5 groups. In this section, some of the results from the conducted reviews will be stated. Table 10 summarizes the reviewed studies according to a taxonomy organized to capture both their technical bases and practical application fields.

The "quantified metrics" column shows quantifiable results wherever feasible, e.g., percentage decreases in latency, energy efficiency, throughput, or detection accuracy. Including these points adds more analytical insight to the comparison so readers can make comparable empirical performance implications of various methods within real-world settings.

The results from the table show that blockchain is used in various fields, including industry, healthcare, supply chain, and IoT.

Because many BIoT solutions overlap across many dimensions, a study may be classified with multiple labels. The first-order category is assigned based on the foremost design objective or the general theme of evaluation. Secondary labels represent secondary attributes or functionalities. For example, an industrial IoT multi-tiered architecture employing erasure coding and optimized PBFT would be classified primarily under "Deployment Architecture – Multi-tier" and secondarily under "Data Management Strategy – Hybrid" and "Consensus Mechanism Family – Optimized PBFT."

To quantify and analyze co-occurrences in categories, a binary incidence matrix was constructed with studies on rows and classification categories as columns. Overlap coefficients (Jaccard similarity) were then computed to determine co-occurrence patterns. This indicates that lightweight consensus protocols usually co-occur with edge/fog deployments, while storage optimization techniques (off-chain and hybrid) co-occur with fault-tolerant consensus processes in industrial and healthcare applications.

From Table 10's perspective, the trends have the following practical implications:

High-overlap clusters (e.g., edge deployment + lightweight consensus + healthcare domain) suggest extensively examined category pairs with evidence of feasibility.

Low-overlap pairs (e.g., hybrid storage and DAG-based consensus in smart cities) suggest unexamined design spaces and may reflect innovation potential.

Certain reliability objectives, PBFT, overindicate multi-category overlaps so that resilience is an intrinsic issue for BIoT research.

The conclusion drawn from the table is that the implementation of the introduced mechanisms brings about improved efficiency, reduced latency, increased security and reliability, enhanced protection of sensitive data, etc.

The authors suggest that by storing sensor data on the blockchain through transactions, the system can achieve security with fewer resources, as the blockchain infrastructure inherently provides essential security features. Given that sensors and edge devices typically have limited computing capabilities, the integration of additional nodes with higher computational power is necessary to handle intensive computing tasks.

Using a substantial volume of high-quality shared data and a robust blockchain-based distributed computing system, blockchain could potentially enable the integration of AI with IoT systems [81,82]. AI methodologies play a vital role in enhancing automated tasks such as scheduling and energy transactions within IoT environments, thereby reinforcing edge computing scalability and increasing compute capacity for IoT data processing [83,84]. In this context, IoT devices execute learning models locally and exchange updates with various decentralized fusion servers, which subsequently share their IoT device learning models before conducting global model aggregation [85,86]. Federated learning enables users and end devices to retain their local data sets and only transmit trained models to the central server [87].

Smart contract–driven security solutions require minimal changes to existing network infrastructures, leveraging blockchain's inherent trustless, decentralized, auditable, and tamper-resistant nature along with its programmable capabilities. Some studies combine blockchain capabilities with the flexible nature of smart contracts. This combination makes it possible to create blockchain-based solutions for IoT applications that deal with permission, authentication, and access control. One of the main tools is the programmability of smart contracts and the decentralized, trustless nature of blockchain technology. These components are essential for studies aimed at smart contract-driven security solutions tailored to the internet. Additionally, these investigations make use of blockchain smart contracts' tamper-resistance to maintain data integrity, safeguard IoT devices, and guarantee the preservation of evidence [88].

Not only do the surveyed studies confirm the viability of integration, but they also suggest several designs to facilitate it. Nevertheless, numerous unresolved issues and challenges persist for researchers, including limitations of IoT devices, big data analysis, and other previously identified hurdles associated with BIoT integration. An obstacle in deploying blockchain as a service for IoT lies in the hosting environment, as edge devices often face constraints in computational resources and available bandwidth, potentially necessitating cloud or fog hosting solutions (Table 11).

One of the primary limitations or drawbacks in such models is consensus algorithms, as employing generic algorithms may hinder the system from operating at its optimal performance level. Ongoing research focuses on developing consensus protocols to enhance the scalability of integration. Given the resource-constrained nature of IoT devices in IoT applications, direct participation in consensus mechanisms like PoW may be unsuitable. While a wide array of consensus protocol proposals exists, they are generally nascent and require further testing. Different consensus protocols inside the blockchain network have different resource requirements, which frequently call for assigning these responsibilities to gateways or unrestricted devices that are competent to do them. As an alternative, off-chain technologies that transfer data outside of the blockchain to reduce latency might be a good choice [89]. Research endeavors should leverage the IoT's distributed nature and global reach to adapt consensus mechanisms in IoT environments.

A literature review of blockchain in IoT has been performed from the beginning until July 2024, and Fig. 3 shows the result. Among them, 10 % of the research work pertained to water management, 20 % of the work addressed supply chain management, and 7 % of them were

Table 10
Enhanced Comparison of Blockchain in IoT Systems.

Year	Ref	Consensus Mechanism	Fault-Tolerant Design	Data Integrity Technique	Application	Quantified Metrics
2020	[35]	PoA (low-power, fast mining)	×	ENODE-based encryption, secure time sync	Industrial IoT	High security, 40 % CPU load increase
2022	[36]	HDPoA (Honesty-based DPoA)	Authority and worker nodes' roles	Blockchain immutability and validation	Smart environment	10 % faster detection
2024	[37]	PoS	Lagrange coded computing	Cosine-similarity validation	Industrial IoT	Improved accuracy, reduced latency, enhanced data integrity
2020	[38]	Proof-of-learning — based on loss reduction in training	×	Blockchain ensures verifiable, tamper-proof sharing of models	Cloud-edge-IoT	20 % reduction in computation overhead
2023	[39]	Modified PoV consensus	Consortium model with low-latency design	IPFS + hybrid encryption (elliptic curve cryptography, physical unclonable function)	Industrial IoT	High detection accuracy, reduced latency, improved scalability
2021	[40]	Hybrid: HDPoA (Honesty-based PoA + lightweight PoW)	Leader–worker node model with round-robin validation	On-chain logging, node honesty levels, and secure transactions	IoT systems	25 % resource consumption reduction
2020	[41]	Lightweight, permissioned (likely BFT-type)	×	Blockchain-based traceable data sharing	Industrial IoT	30 % improvement in process efficiency
2020	[42]	BFT-DPoS consensus in a permissioned edge blockchain	×	Immutable ledger of transactions; encrypted credentials and signatures for trading	Wireless edge systems	15 % increase in energy efficiency
2022	[43]	Permissioned blockchain and smart contracts	Smart contract monitors and blocks attacks			
Immutable ledger with cryptographic proofs	Organizational IoT	20 % reduction in false positives				
2020	[44]	Ethereum PoW consensus	Decentralized oracles (multi-sensor voting)	Immutable blockchain ledger, cryptographic verification	IoT monitoring	33 % transaction cost reduction
2020	[47]	×	Block lifetime, lightweight blocks, block subdivision	Block retention, block packaging	IoT devices	Block lifetime (min/hours), latency (ms), storage overhead (MB), energy consumption (J)
2021	[48]	Hyperledger Fabric (endorsement + ordering)	Peer replication in Fabric	Hashing, smart contracts, encryption	Healthcare	Not reported
2022	[49]	Blockchain-based distributed consensus (e.g., PoW or PBFT)	SDN-based traffic rerouting, distributed ledger redundancy	Blockchain immutability, secure communication protocols, AI-based validation	IoT networks	40 % reduction in energy consumption
2023	[50]	DAG-based asynchronous validation	Distributed prophecy machine and DAG	SHA-256, zero-knowledge proofs, IPFS	IoT security	10.5 % improvement in block processing
2022	[51]	BFT algorithm, decentralized edge architecture	BFT algorithm, decentralized edge architecture	Cryptographic hashing, permission control	IoT devices	Latency measurements, throughput evaluation, system availability under fault conditions
2021	[55]	Digital signatures, encryption, immutable ledgers, digital identity access control	×	Digital signatures, encryption, immutable ledgers, digital identity access control	Industry	27 % error detection rate
2020	[56]	Hyperledger Fabric endorsement & ordering	×	Cryptographic hashing, asymmetric encryption, smart contracts	Food supply chain	40 % reduction in authentication time
2024	[57]	×	×	Identity-based encryption + blockchain	Cloud IoT	12 % increase in detection accuracy
2021	[58]	Blockchain for trust and authentication; public ledger for verified participants	×	Blockchain ensures tamper-proof updates and model validation	Industrial IoT	Detection accuracy ≈ 0.93, detection rate ≈ 0.96; improved energy efficiency and longer network lifetime
2024	[59]	Raft (Hyperledger Fabric)	×	Hashing, blockchain, IPFS	IoT devices	>90 % accuracy (vs. 75–85 % in previous models)
2022	[60]	Hyperledger Fabric consensus protocol	×	Blockchain as distributed ledger + homomorphic encryption + secure searchable encryption	Healthcare	Reduced confirmation time compared to benchmark models; enhanced throughput and security
2023	[61]	×	×	Cryptographic hashing of data blocks, immutable ledger, smart contracts for access control	Agriculture	SVM accuracy: 97.73 %

(*continued on next page*)

Table 10 (*continued*)

Year	Ref	Consensus Mechanism	Fault-Tolerant Design	Data Integrity Technique	Application	Quantified Metrics
2020	[62]	×	×	Immutable blockchain ledger with cryptographic receipts; signed input/ output hashes for auditing		
2023	[63]	PoA via edge nodes	×	Zero-knowledge proof, blockchain, IPFS, smart contracts	Healthcare	25 % increase in detection speed
2020	[64]	RAFT (lightweight, crash-tolerant)	Tolerates 50 % crash faults	TLS + endorsement + digital signatures	IoT devices	Response time < 100 s for 1000 transactions
RAM usage < 300 MiB for 1000 transactions						
2020	[65]	Block validation by cluster heads (LSB structure)	Enhanced block validation for performance	EC-ElGamal encryption for transaction security Genetic algorithm-based SHA-384 hashing	IoT devices	42 % faster processing; 37 % storage cost reduction
2020	[66]	×	Two-ledger system (urgent vs. normal) to manage transmission delays	Blockchain (lightweight & conventional), SHA-256 hashing, ledgers	Smart dust IoT	Up to 96 % transmission time improvement
2021	[67]	Apache Kafka + federated voting	Sharding-based replication, Reactive Streaming	Digital signatures, Off-chain proof storage	IoT devices	48 % increase in throughput
2021	[68]	Hyperledger Fabric (endorsing peers, ordering service)	×	Blockchain ledger & smart contracts for tamper-resistance	IoT applications	27 % security enhancement
2021	[69]	Improved PBFT (Incentive-based)	Reed-Solomon erasure coding	RS-based Recovery	Smart medicine	44 % reduced latency
2022	[70]	Lightweight blockchain consensus (possibly simplified PBFT or custom protocol)	Decentralized architecture; node redundancy	Cryptographic hashing, secure logging; blockchain immutability	Healthcare	21 % faster access; latency
2023	[71]	Ethereum's PoW consensus in blockchain	LRA serves as validators/ full nodes; edge/MEC nodes for distributed validation and redundancy	Merkle tree for lightweight client verification; cryptographic hashing for certificate validation	IoT devices	47 % faster certification
2023	[72]	×	×	Blockchain ledger ensuring tamper-proof access control records; cryptographic verification using HCC	IoT devices	Reduced computation time and communication cost compared to previous schemes
2022	[74]	Local and global consensus tiers	Feature redundancy + probing tests	Immutable blockchain records with smart contracts	IoT devices	50–100 trust events/ community
2022	[75]	PBFT (multi-entry) with RTS/CTS	Leader rotation, queue reduction, tiered clusters	Tiered validation and deterministic linking	Industrial IoT	<100 ms latency; 5-tier setup
2022	[76]	×	×	Intelligent reflecting surface-supported physical layer security and secrecy rate	Smart grid	20 % improved energy efficiency
2023	[77]	GH-PBFT	PBFT with 2f+1 message confirmations	CLS, digital signatures, message hashing	IoT systems	Not reported
2024	[78]	Federated blockchain consensus	Asynchronous federated learning	Encrypted models on blockchain	Industrial IoT	30 % model convergence stability
2024	[79]	PoC, public blockchain layer	Layered clustering, isolation	Symmetric keys, blockchain hash	IoT applications	1000–2000 TPS (lower layers)
2024	[80]	×	Erasure coding (Reed-Solomon)	Blockchain immutability + coding	IoT systems	86.3 % reduction in storage overhead, 15.8 % improvement over MLDC, 7.35 % lower cross-tier query cost

agricultural applications. Despite the fact that healthcare-related applications comprised a very significant proportion (27 %) of the studies reviewed, industrial IoT applications comprised the highest proportion at 32 %. This indicates that there is more focus on using blockchain in industrial automation, manufacturing security, and process optimization in smart factories.

The IoT has its own characteristics and challenges, such as centralization, security and privacy problems, and problems related to big data management. The integration of IoT with blockchain technology has solved many of its problems and has added features such as reliability and energy reduction to IoT networks. The outcome of combining blockchain technology with the IoT is depicted in Fig. 4.

The BIoT methodology instills trust among interconnected devices by leveraging its robust security features. Only authenticated devices are permitted to engage within the network, with each transaction block subject to verification by miners before inclusion in the blockchain [90]. Securing information and communications through blockchain transactions enhances overall security, as blockchain processes device message exchanges as validated transactions via smart contracts, thereby fortifying inter-device communications [91,92].

While the reviewed papers present promising solutions to enhance security, privacy, and scalability in BIoT systems, they usually have significant trade-offs. Public blockchains, for instance, offer high security and transparency at the expense of high latency and computation

Table 11
Quality assessment of selected BIoT studies.

Ref.	Architectural Novelty	Consensus/Fault tolerance/Integrity mechanisms	Quantitative performance criteria	Experimental validation	Carity/ Reproducibility	Total Score
[35]	4/4	3/4	2/4	4/4	3/4	16/20
[36]	4/4	4/4	4/4	4/4	3/4	19/20
[37]	4/4	3/4	3/4	3/4	2/4	15/20
[38]	4/4	4/4	3/4	3/4	3/4	17/20
[39]	4/4	4/4	2/4	4/4	3/4	17/20
[40]	4/4	4/4	4/4	4/4	3/4	19/20
[41]	4/4	4/4	3/4	4/4	3/4	18/20
[42]	4/4	3/4	4/4	3/4	3/4	17/20
[43]	3/4	2/4	4/4	3/4	3/4	15/20
[44]	4/4	3/4	4/4	4/4	3/4	18/20
[47]	4/4	3/4	3/4	4/4	3/4	17/20
[48]	3/4	4/4	3/4	3/4	3/4	16/20
[49]	4/4	4/4	4/4	4/4	3/4	19/20
[50]	4/4	3/4	3/4	3/4	3/4	16/20
[51]	3/4	4/4	4/4	4/4	3/4	18/20
[55]	3/4	4/4	4/4	4/4	3/4	18/20
[56]	2/4	3/4	3/4	3/4	3/4	14/20
[57]	3/4	1/4	4/4	3/4	3/4	14/20
[58]	3/4	2/4	4/4	3/4	3/4	15/20
[59]	4/4	3/4	3/4	3/4	4/4	17/20
[60]	4/4	4/4	4/4	4/4	3/4	19/20
[61]	4/4	3/4	3/4	3/4	4/4	17/20
[62]	3/4	3/4	4/4	3/4	3/4	16/20
[63]	4/4	4/4	4/4	4/4	3/4	19/20
[64]	4/4	4/4	4/4	3/4	3/4	18/20
[65]	4/4	4/4	4/4	3/4	3/4	18/20
[66]	3/4	2/4	3/4	3/4	3/4	14/20
[67]	3/4	3/4	4/4	4/4	3/4	17/20
[68]	4/4	3/4	3/4	3/4	4/4	17/20
[69]	4/4	4/4	4/4	3/4	3/4	18/20
[70]	4/4	4/4	4/4	4/4	3/4	19/20
[71]	3/4	3/4	4/4	2/4	4/4	16/20
[72]	3/4	3/4	4/4	2/4	4/4	16/20
[74]	4/4	4/4	4/4	4/4	3/4	19/20
[75]	4/4	4/4	4/4	3/4	3/4	18/20
[76]	4/4	4/4	4/4	3/4	4/4	19/20
[77]	4/4	3/4	3/4	3/4	3/4	16/20
[78]	4/4	4/4	3/4	4/4	3/4	18/20
[79]	3/4	3/4	4/4	3/4	3/4	16/20
[80]	4/4	3/4	4/4	4/4	3/4	18/20

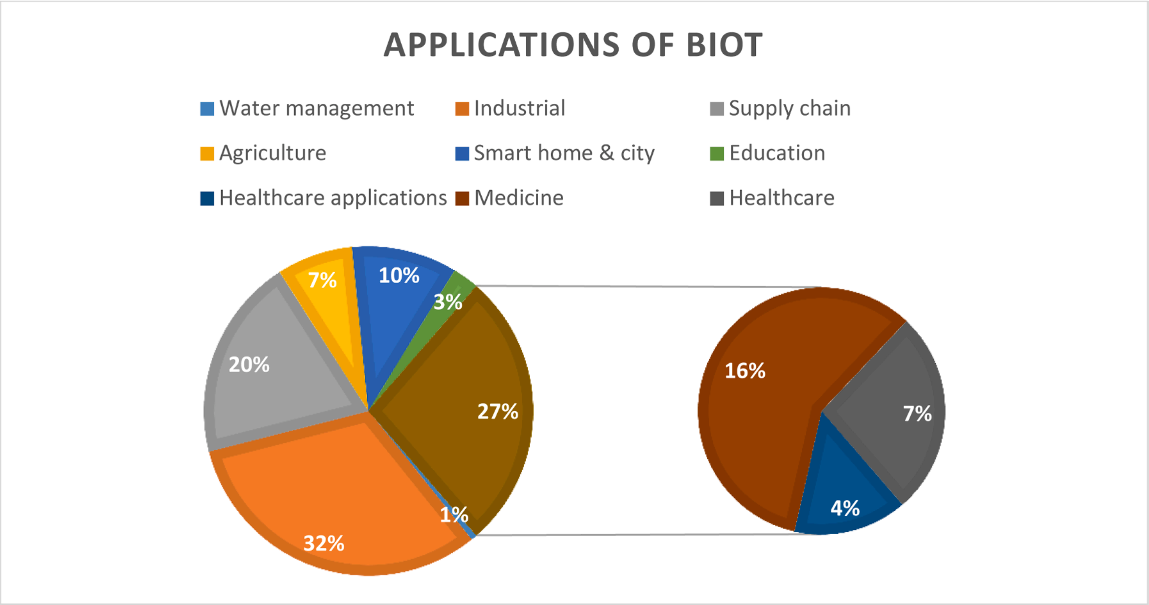

Fig. 3. Application area of BIoT until July 2024.

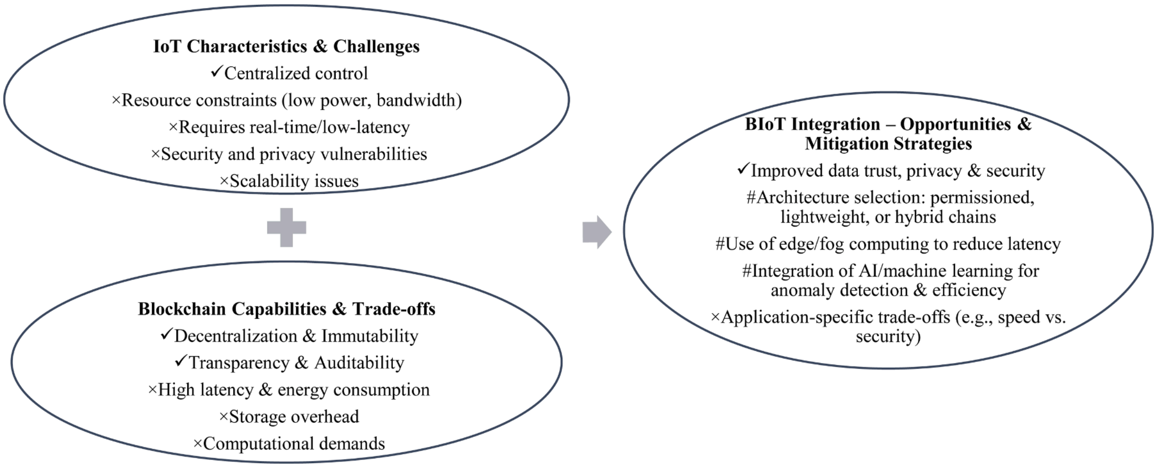
IoT Characteristics & Challenges
✓Centralized control
×Resource constraints (low power, bandwidth)
×Requires real-time/low-latency
×Security and privacy vulnerabilities
×Scalability issues
Blockchain Capabilities & Trade-offs
✓Decentralization & Immutability
✓Transparency & Auditability
×High latency & energy consumption
×Storage overhead
×Computational demands
BIoT Integration – Opportunities & Mitigation Strategies
✓Improved data trust, privacy & security
#Architecture selection: permissioned, lightweight, or hybrid chains
#Use of edge/fog computing to reduce latency
#Integration of AI/machine learning for anomaly detection & efficiency
×Application-specific trade-offs (e.g., speed vs. security)

Fig. 4. Integration of IoT and blockchain technology.
Legend: ✓ = Advantage × = Disadvantage # = Trade-off / Balance required.

overhead, making them less desirable for real-time IoT systems. Conversely, lightweight or permissioned blockchains realize lower energy consumption and faster transaction speed but may be less tolerant of network-scale attacks. Similarly, incorporating machine learning improves the intelligence of the system, but with increased computational demands [93]. The selection of an optimal architecture is therefore application-dependent, based on the trade-off between performance, scalability, and security.

6. Challenges and future works

The IoT ecosystem grapples with various vulnerabilities related to confidentiality, privacy, and data integrity, prompting ICT researchers and developers to incorporate “security by design” principles to address these challenges. Smart contracts allow for transaction authorization and automation, while blockchain technology offers authenticity, non-repudiation, and integrity by default. A viable strategy to solve important concerns like IoT data security and privacy—which are crucial for promoting the widespread use of IoT technologies—is the integration of blockchain technology with IoT systems.

Despite the promising advantages and the envisioned bright future of BIoT, the analysis identifies specific research avenues and challenges for further advancing lightweight blockchain solutions.

Privacy leakage: Transaction records kept in blockchains can have some degree of data privacy control thanks to measures built into blockchain technologies. To provide a certain level of anonymity, Bitcoin transactions, for example, employ IP addresses rather than individuals’ real identities. In addition, Bitcoin creates one-time accounts in order to improve user privacy [94]. However, there are weaknesses in these defense mechanisms. The research outlined in demonstrates that user pseudonyms can be deciphered through data learning and inference from multiple transactions associated with a single user. Besides, storing transaction data in its entirety on the blockchain may pose potential privacy risks, as highlighted in.

Data retrieval: Most publications do not include the methodology for retrieving the data. Due to the intricacies involved in obtaining data in blockchain-based systems, retrieval procedures might take either on- or off-chain. Data extraction from encrypted files and the usage of searchable encrypted image files are essential since picture files in the healthcare sector are encrypted and stored on-chain. However, there is currently a dearth of research in this field, necessitating further investigation [24].

Rapid field testing: In the foreseeable future, the optimization of various blockchain types relevant to diverse applications will become imperative. Integration of blockchain with IoT systems necessitates selecting a blockchain that aligns with specific requirements. Consequently, developing a mechanism to evaluate different blockchains becomes essential [95]. This process should be divided into two key stages: standardization and testing. During the standardization phase, comprehensive analysis and agreement on all requirements after understanding supply chains, markets, products, and services are crucial. Subsequently, any developed blockchain should undergo testing against the agreed criteria to validate its functionality. The testing phase entails evaluating various criteria such as security, privacy, throughput, energy efficiency, blockchain capacity, latency, and usability, among others [96].

Scalability: Both machine learning and blockchain encounter scalability challenges related to processing and communication costs. The integration of many machine learning algorithms incurs additional processing and communication costs with the surge in data volume, a common scenario in IoT networks. Similarly, blockchain performance deteriorates with an increasing number of users and network nodes [97,98]. For instance, the Ethereum blockchain typically handles only 12 transactions per second, which is inadequate for conventional IoT applications that witness millions of transactions per second [99,100].

Edge Computing and Mobility: On a larger scale, satellite networks impose considerable delays in vertical transmissions spanning aerial, terrestrial, and space domains. Conversely, high-altitude platforms within aerial access networks support edge caching and data processing, thereby lowering computational demands and minimizing latency compared to satellite networks while ensuring essential service delivery. As a result, a rigorous exploration into edge caching is necessary, focusing on resource distribution, localization, computational efficiency, power optimization, and other pertinent aspects [101].

Data Storage: On the other hand, the IoT system is recognized as a significant source of big data. Storage capacity poses a critical challenge for blockchain technology. The total size of the Bitcoin blockchain is approximately 150 gigabytes, and the Ethereum blockchain spans around 400 gigabytes. It is imperative to store all blockchain blocks, as IoT devices rely on previous blocks to validate transactions from other devices and generate new transactions. IoT devices create enormous amounts of data, estimated in zettabytes, which are too expensive to store on the blockchain. Blockchain data storage is still complicated and expensive, even if the convergence of IoT with blockchain removes the need for a centralized server to store IoT data. Therefore, more investigation is necessary to examine novel strategies for resolving this problem [102,103]. Blockchain architecture is not designed to handle extensive data volumes.

Latency and throughput: Achieving consensus for transaction validation in public blockchains necessitates a substantial number of participants, each requiring access to the entire network to verify transactions and reach an agreement. This process results in latency challenges in public blockchains and introduces security risks by granting unlimited network access. Enhancing blockchain throughput for shared use demands significant efforts to overcome these challenges and position blockchain as a leading protocol [104].

Trusty framework: Establishing a comprehensive trust framework or infrastructure is crucial to meet the prerequisites for integrating blockchain into IoT systems. Numerous innovative approaches to trust-related issues rely on cross-domain regulations and controls. Governments might, for example, set up blockchain infrastructure to facilitate use cases that benefit the general public [96].

Combination of AI and IoT: The integration of AI, IoT, Big Data, and blockchain has the potential to transform various aspects of contemporary life, offering robust, secure, and efficient solutions to complex issues. AI can leverage the vast data streams from IoT devices to enhance customer service, optimize internal operations, and maximize resource utilization [105]. Recent successes in applying machine learning algorithms, particularly deep learning algorithms, across diverse domains underscore their effectiveness. Though it is essential to carefully choose learning classes (including unsupervised, supervised, and reinforcement learning) and matching algorithms (like K-means clustering and SVMs), deploying these algorithms in cloud data warehouses might uncover interesting patterns. Integrating machine learning capabilities into hybrid blockchain setups necessitates further research to unlock their potential fully, emphasizing a systems engineering approach [27,106].

Resiliency against Combined Attacks: Numerous security solutions have been proposed in the literature to address blockchain-based IoT security challenges, each tailored to mitigate specific security threats. A pivotal consideration is designing a resilient security solution capable of combating combined attacks while ensuring practical implementation feasibility, especially for resource-constrained IoT devices [107].

Availability: An essential issue in data exchange revolves around optimizing the utility of data models derived from raw data, irrespective of specific computational tasks and machine learning algorithms [108].

Security of the blockchain: Investigating strategies to enhance blockchain performance for alignment with IoT applications remains an open area of inquiry. Furthermore, comprehending the security landscape of the blockchain platform itself is a critical undertaking. While blockchain is commonly harnessed to bolster the security of IoT applications, the blockchain platform, being a form of software, presents its security vulnerabilities. Notably, researchers have revealed vulnerabilities in smart contracts that could have severe repercussions, particularly in payment applications and other contexts. A thorough exploration of blockchain platform security demands a systematic investigation.

It is worth highlighting that current research endeavors exploring the utilization of blockchain for IoT applications are still in their nascent stages, with a predominant focus on proof-of-concept studies.

Standardization for Comparative Evaluation: Future work must address the development of standardized benchmarks for BIoT, with well-defined metrics and baseline circumstances to facilitate consistent, reproducible, and equitable comparisons between blockchain-IoT platforms.

7. Conclusions and limitations

This research examined ongoing attempts to leverage blockchain-based systems to develop and deploy services involving IoT functionality. The study aims to address a set of issues, including information security, data privacy, data harmonization, and regulating transactions. It establishes through literature search the mechanism for integrating both technologies into four types:

1) consensus mechanisms, 2) fault-tolerant designs, 3) data integrity techniques, 4) multi-layered architectures, and 5) lightweight blockchain-based mechanisms.

The review was able to verify that this approach enhances the security of the IoT environment by enabling the development of smart contracts and secure data storage, providing a decentralized platform for applying learning algorithms, and offering protection to data in cloud systems. Additionally, combining IoT with blockchain technology minimizes latency, enables easy communication, and reduces energy consumption.

The following are the limitations of the studies reviewed: Despite more advancements, not much effort has been directed toward addressing the scalability issues of blockchain-based low-power wireless sensor networks, a pressing problem. Also, one of the major flaws of the PoW consensus protocol, which is the most popular consensus algorithm, is resource inefficiencies, with nodes possessing high hash power being more likely to mine a block. This leads to considerable investments in hardware upgrades, once again boosting the consumption of resources. In order to solve these problems, upcoming operations need to emphasize enhancing interoperability among various blockchain networks and IoT networks so that digital identities can be seamlessly connected on numerous platforms. Until now, interoperability among existing solutions is limited, which means there is a critical need for more research and development for cross-platform compatibility. Also, energy consumption and processing overhead remain significant challenges in resource-constrained IoT environments and require further optimization [109]. Scalability issues in public blockchains, such as high latency and high transaction fees, also limit their application in large-scale IoT networks. Moreover, there is no standardized model of security, and no unified model of security for IoT blockchain uses, resulting in inconsistency in protecting IoT environments. Finally, there is still compliance with regulations and no overarching mechanism to guarantee that blockchain IoT systems comply with rules in healthcare, food safety, and other spaces.

Besides, some of the key challenges that have been realized are the compromise between latency and security, where blockchain protocols like PBFT are accompanied by high latency, which makes them unsuitable for real-time IoT applications. Consensus efficiency is also a challenge, where current consensus protocols are energy-consuming, which is a challenge in IoT environments that require power efficiency. Further, the absence of cross-chain interoperability is a challenge in integrating different blockchain solutions into current IoT networks. Finally, high deployment costs are a significant hindrance, e.g., infrastructure and hardware investment.

Future studies need to overcome these challenges by exploring energy-efficient blockchain platforms, developing standardized security protocols, scalable and interoperable systems, and cost-effective deployments. AI and machine learning integration to identify anomalies in real-time and enhance security for IoT networks will also be crucial in overcoming the challenges.

CRediT authorship contribution statement

Xin Sun: Data curation, Conceptualization. **Xinglong Yu:** Funding acquisition, Formal analysis. **Qinlu Huang:** Resources, Investigation. **Zhigang Wang:** Writing – review & editing, Supervision. **Jiahu Guo:** Visualization, Software. **Zhihao Huang:** Writing – original draft, Methodology. **Fei Xie:** Writing – original draft, Validation.

Declaration of competing interest

No conflict of interest exists.

We wish to confirm that there are no known conflicts of interest associated with this publication.

Funding

No Funding.

Data availability

This study is a review article and does not involve the generation or analysis of new datasets. All data supporting the findings of this study are obtained from previously published sources, which are cited in the reference list.

References

[1] R. Mohammed, R. Alubady, A. Sherbaz, Utilizing blockchain technology for IoT-based healthcare systems, in: Journal of Physics: Conference Series, IOP Publishing, 2021.
[2] Q. Zhang, et al., A group key agreement protocol for intelligent internet of things system, Int. J. Intell. Syst. 37 (1) (2022) 699–722.
[3] S. Basudan, A scalable blockchain framework for secure transactions in IoT-based dynamic applications, IEEE Open J. Commun. Soc. (2023).
[4] M. Bhandary, M. Parmar, D. Ambawade, A blockchain solution based on directed acyclic graph for IoT data security using IoTA tangle, in: 2020 5th International Conference on Communication and Electronics Systems (ICCES), IEEE, 2020.
[5] H.D. Zubaydi, P. Varga, S. Molnár, Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review, Sensors 23 (2) (2023) 788.
[6] H.-N. Dai, Z. Zheng, Y. Zhang, Blockchain for Internet of Things: A survey, IEEe Internet. Things. J. 6 (5) (2019) 8076–8094.
[7] Z. Wan, W. Liu, H. Cui, HIBEChain: A hierarchical identity-based blockchain system for large-scale IoT, IEEe Trans. Dependable Secure Comput. 20 (2) (2022) 1286–1301.
[8] O. Alsamarah, K.A. Alshare, P.L. Lane, Determinants of individual's intention to use the internet of things for smart home technology: a cultural moderating effect, Int. J. Mob. Commun. 21 (3) (2023) 316–340.
[9] J.H. Ziegeldorf, O.G. Morchon, K. Wehrle, Privacy in the Internet of Things: threats and challenges, Secur. Commun. Netw. 7 (12) (2014) 2728–2742.
[10] A. Rejeb, et al., Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions, Internet Thing Cyber-Phys. Syst. 4 (2024) 1–18.
[11] V. Dedeoglu, et al., 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.
[12] B.K. Chaurasia, B. Chakraborty, D. Sadhya, Trust computation in VNs using blockchain, Wireless Networks 31 (3) (2025) 1989–2003.
[13] M.S. Peelam, et al., Unlocking the Potential of Interconnected blockchains: a Comprehensive Study of Cosmos Blockchain Interoperability, IEEE Access, 2024.
[14] S. Woo, J. Song, S. Park, A distributed oracle using Intel SGX for blockchain-based IoT applications, Sensors 20 (9) (2020) 2725.
[15] D. Kumar, et al., Roadmap for integrating blockchain with Internet of Things (IoT) for sustainable and secured operations in logistics and supply chains: decision making framework with case illustration, Technol. Forecast. Soc. Change 196 (2023) 122837.
[16] S. Pešić, et al., Hyperledger fabric blockchain as a service for the IoT: proof of concept, in: Model and Data Engineering: 9th International Conference, MEDI 2019, Springer, Toulouse, France, 2019. Proceedings 9.
[17] S. Srivastava, et al., Blockchain-based trust management for data exchange in internet of vehicle network, Multimed. Tools. Appl. 84 (8) (2025) 4837–4855.
[18] M. Conoscenti, A. Vetro, J.C. De Martin, Blockchain for the Internet of Things: A systematic literature review, in: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), IEEE, 2016.
[19] S.K. Lo, et al., Analysis of blockchain solutions for IoT: A systematic literature review, IEEe Access. 7 (2019) 58822–58835.
[20] N.K. Tran, M.A. Babar, J. Boan, Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs, J. Netw. Comput. Appl. 173 (2021) 102844.
[21] M. Hussain, et al., Blockchain-based IoT devices in Supply Chain management: A systematic literature review, Sustainability. 13 (24) (2021) 13646.
[22] D. Stefanescu, et al., A systematic literature review of lightweight blockchain for IoT, IEEe Access. 10 (2022) 123138–123159.
[23] A. Akinbi, Á. MacDermott, A.M. Ismael, A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models, Forensic Sci. Int.: Digit. Invest. 42 (2022) 301470.
[24] E.M. Adere, Blockchain in healthcare and IoT: A systematic literature review, Array 14 (2022) 100139.
[25] M.H. Ahmed, Integration of blockchain with the internet of things: A systematic review, Sci. Open Preprints (2022).
[26] A. Ivić, et al., The challenges and opportunities in adopting AI, IoT and blockchain technology in E-government: A systematic literature review, in: 2022 International Conference on Communications, Information, Electronic and Energy Systems (CIEES), IEEE, 2022.
[27] A. Alkhateeb, et al., Hybrid blockchain platforms for the internet of things (IoT): A systematic literature review, Sensors 22 (4) (2022) 1304.
[28] M.J. Page, et al., The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, BMJ 372 (2021).
[29] E.-M. Schön, J. Thomaschewski, M.J. Escalona, Agile Requirements Engineering: A systematic literature review, Comput. Stand. Interfaces. 49 (2017) 79–91.
[30] S. Auer, et al., Towards blockchain-IoT based shared mobility: car-sharing and leasing as a case study, J. Netw. Comput. Appl. 200 (2022) 103316.
[31] J.P. Queralta, T. Westerlund, Blockchain for mobile edge computing: consensus mechanisms and scalability. Mobile Edge Computing, Springer, 2021, pp. 333–357.
[32] Y. Xiao, et al., A survey of distributed consensus protocols for blockchain networks, IEEE Commun. Surv. Tutor. 22 (2) (2020) 1432–1465.
[33] H. Luo, et al., Symbiotic blockchain consensus: cognitive backscatter communications-enabled wireless blockchain consensus, IEEE/ACM Trans. Netw. (2024).
[34] M.M. Yakubu, et al., A systematic literature review on Blockchain Consensus Mechanisms' Security: applications and open challenges, Comput. Syst. Sci. Eng. 48 (6) (2024).
[35] S. Misra, et al., Blockchain at the edge: performance of resource-constrained IoT networks, IEEE Trans. Parall. Distrib. Syst. 32 (1) (2020) 174–183.
[36] S.M. Alrubei, E. Ball, J.M. Rigelsford, A secure blockchain platform for supporting AI-enabled IoT applications at the edge layer, IEEe Access. 10 (2022) 18583–18595.
[37] Y. Chen, et al., Leveraging blockchain and coded computing for Secure Edge collaborate learning in industrial IoT, in: 2024 33rd International Conference on Computer Communications and Networks (ICCCN), IEEE, 2024.
[38] C. Qiu, et al., Networking integrated cloud–edge–end in IoT: A blockchain-assisted collective Q-learning approach, IEEe Internet. Things. J. 8 (16) (2020) 12694–12704.
[39] A.S. Hosen, et al., SECBlock-IIoT: a secure blockchain-enabled edge computing framework for industrial Internet of Things, in: Proceedings of the Third International Symposium on Advanced Security on Software and Systems, 2023.
[40] S.M. Alrubei, E. Ball, J.M. Rigelsford, The use of blockchain to support distributed AI implementation in IoT systems, IEEe Internet. Things. J. 9 (16) (2021) 14790–14802.
[41] T. Kumar, et al., BlockEdge: blockchain-edge framework for industrial IoT networks, IEEe Access. 8 (2020) 154166–154185.
[42] X. Lin, et al., Blockchain-based incentive energy-knowledge trading in IoT: joint power transfer and AI design, IEEe Internet. Things. J. 9 (16) (2020) 14685–14698.
[43] M. Sarhan, et al., HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection, Comput. Electr. Eng. 103 (2022) 108379.
[44] N. Mhaisen, et al., To chain or not to chain: A reinforcement learning approach for blockchain-enabled IoT monitoring applications, Future Gener. Comput. Syst. 111 (2020) 39–51.
[45] R. Guo, et al., A hierarchical byzantine fault tolerance consensus protocol for the internet of things, High-Confid. Comput. 4 (3) (2024) 100196.
[46] Xu, R., et al., Microchain: A hybrid consensus mechanism for lightweight distributed ledger for IoT. arXiv preprint arXiv:1909.10948, 2019.
[47] S. Garlapati, Trade-offs in the design of blockchain of finite-lifetime blocks for edge-iot applications, in: 2020 29th International Conference on Computer Communications and Networks (ICCCN), IEEE, 2020.
[48] F. Jamil, et al., Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms, Sensors 21 (5) (2021) 1640.
[49] S.A. Latif, et al., AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems, Comput. Commun. 181 (2022) 274–283.
[50] J. Cai, et al., GTxChain: A secure IoT smart blockchain architecture based on graph neural network, IEEe Internet. Things. J. 10 (24) (2023) 21502–21514.
[51] Y. Wu, et al., Bring trust to edge: secure and decentralized IoT framework with BFT and permissioned blockchain, in: 2022 IEEE International Conference on Edge Computing and Communications (EDGE), IEEE, 2022.
[52] S.S. Hameedi, O. Bayat, Improving IoT data security and integrity using lightweight blockchain dynamic table, Appl. Sci. 12 (18) (2022) 9377.
[53] Q.-u.-A. Arshad, et al., Blockchain-based decentralized trust management in IoT: systems, requirements and challenges, Complex. Intell. Systems. 9 (6) (2023) 6155–6176.
[54] Omar, Y.A., Blockchain-enabled data integrity in wireless sensor networks.
[55] Z. Shahbazi, Y.-C. Byun, Integration of blockchain, IoT and machine learning for multistage quality control and enhancing security in smart manufacturing, Sensors 21 (4) (2021) 1467.
[56] P.W. Khan, Y.-C. Byun, N. Park, IoT-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning, Sensors 20 (10) (2020) 2990.
[57] V. Saravanan, et al., IoT-based blockchain intrusion detection using optimized recurrent neural network, Multimed. Tools. Appl. 83 (11) (2024) 31505–31526.
[58] S. Otoum, I. Al Ridhawi, H. Mouftah, Securing critical IoT infrastructures with blockchain-supported federated learning, IEEe Internet. Things. J. 9 (4) (2021) 2592–2601.
[59] R. Ratnayake, M. Liyanage, L. Murphy, Machine learning for data trust evaluations in blockchain-enabled IoT systems, in: 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), IEEE, 2024.
[60] A. Ali, et al., An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network, Sensors 22 (2) (2022) 572.

[61] N.S. Sizan, et al., Revolutionizing agriculture: an IoT-driven ML-blockchain framework 5.0 for optimal crop prediction, in: 2023 5th International Conference on Sustainable Technologies for Industry 5.0 (STI), IEEE, 2023.

[62] Y. He, et al., Blockchain-based edge computing resource allocation in IoT: A deep reinforcement learning approach, IEEe Internet. Things. J. 8 (4) (2020) 2226–2237.

[63] P. Kumar, et al., A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system, J. Parallel. Distrib. Comput. 172 (2023) 69–83.

[64] A.H. Alkhazaali, A. Oğuz, Lightweight fog based solution for privacy-preserving in IoT using blockchain, in: 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), IEEE, 2020.

[65] J. Guruprakash, S. Koppu, EC-ElGamal and genetic algorithm-based enhancement for lightweight scalable blockchain in IoT domain, IEEe Access. 8 (2020) 141269–141281.

[66] J. Park, K. Park, A two-class data transmission method using a lightweight blockchain structure for secure smart dust iot environments, Sensors 20 (21) (2020) 6078.

[67] E. Bandara, et al., Tikiri—Towards a lightweight blockchain for IoT, Future Gener. Comput. Syst. 119 (2021) 154–165.

[68] X. Qin, et al., LBAC: A lightweight blockchain-based access control scheme for the internet of things, Inf. Sci. (Ny) 554 (2021) 222–235.

[69] C. Li, et al., Lightweight blockchain consensus mechanism and storage optimization for resource-constrained IoT devices, Inf. Process. Manage 58 (4) (2021) 102602.

[70] O. Said, LBSS: A lightweight blockchain-based security scheme for IoT-enabled healthcare environment, Sensors 22 (20) (2022) 7948.

[71] A. Garba, et al., LightCERT4IoTs: Blockchain-based lightweight certificates authentication for IoT applications, IEEe Access. 11 (2023) 28370–28383.

[72] S.S. Ullah, V.A. Oleshchuk, H.S.G. Pussewalage, A Lightweight Access Control Scheme With Attribute Policy For Blockchain-Enabled Internet of Things, SECRYPT, 2023.

[73] Y.E. Oktian, S.-G. Lee, H.J. Lee, Hierarchical multi-blockchain architecture for scalable internet of things environment, Electronics. (Basel) 9 (6) (2020) 1050.

[74] E. Corradini, et al., A two-tier blockchain framework to increase protection and autonomy of smart objects in the IoT, Comput. Commun. 181 (2022) 338–356.

[75] J. Mišić, V.B. Mišić, X. Chang, Optimal multi-tier clustering of permissioned blockchain systems for IoT, IEEe Trans. Veh. Technol. 71 (3) (2022) 2293–2304.

[76] Y. Liu, Z. Su, Y. Wang, Energy-efficient and physical-layer secure computation offloading in blockchain-empowered internet of things, IEEe Internet. Things. J. 10 (8) (2022) 6598–6610.

[77] Z. Dai, Q. Xia, Blockchain for iot scenarios: lightweight three-tier architecture with GH-PBFT consensus, in: Proceedings of the 2023 6th International Conference on Blockchain Technology and Applications, 2023.

[78] X. Wang, et al., Dual-blockchain based multi-layer grouping federated learning scheme for heterogeneous data in industrial IoT, Blockchain: Res. Appl. 5 (3) (2024) 100195.

[79] T.A.A.A.A. Bary, B.M. Elomda, H.A. Hassan, Multiple layer public blockchain approach for Internet of Things (IoT) systems, IEEe Access. 12 (2024) 56431–56438.

[80] X. Xu, et al., MTEC: A multi-tier blockchain storage framework using erasure coding for IoT application, in: Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint International Conference on Web and Big Data, Springer, 2024.

[81] R. Yang, et al., Integrated blockchain and edge computing systems: A survey, some research issues and challenges, IEEE Commun. Surv. Tutor. 21 (2) (2019) 1508–1532.

[82] S. Singh, et al., Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city, Sustain. Cities. Soc. 63 (2020) 102364.

[83] J. Xie, et al., A survey of blockchain technology applied to smart cities: research issues and challenges, IEEE Commun. Surv. Tutor. 21 (3) (2019) 2794–2830.

[84] A. Abdelmaboud, et al., Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions, Electronics. (Basel) 11 (4) (2022) 630.

[85] L. Tan, et al., A blockchain-based access control framework for cyber-physical-social system big data, IEEe Access. 8 (2020) 77215–77226.

[86] Y.I. Alzoubi, et al., Internet of things and blockchain integration: security, privacy, technical, and design challenges, Future Internet. 14 (7) (2022) 216.

[87] P. Wang, et al., Server-initiated federated unlearning to eliminate impacts of low-quality data, IEEe Trans. Serv. Comput. 17 (3) (2024) 1196–1211.

[88] A.H. Lone, R. Naaz, Applicability of blockchain smart contracts in securing internet and IoT: A systematic literature review, Comput. Sci. Rev. 39 (2021) 100360.

[89] G. Sun, et al., Cost-efficient service function chain orchestration for low-latency applications in NFV networks, IEEe Syst. J. 13 (4) (2018) 3877–3888.

[90] Alam, T., Blockchain and its role in the Internet of Things (IoT). arXiv preprint arXiv:1902.09779, 2019.

[91] M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.

[92] A. Reyna, et al., On blockchain and its integration with IoT. Challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190.

[93] Y. Xu, et al., Blockchain-based AR offloading in UAV-enabled MEC networks: A trade-off between energy consumption and rendering latency, IEEe Trans. Veh. Technol. (2025).

[94] M. Zhang, et al., Age-dependent differential privacy, IEEe Trans. Inf. Theory. 70 (2) (2023) 1300–1319.

[95] K. Zanbouri, et al., A GSO-based multi-objective technique for performance optimization of blockchain-based industrial internet of things, Int. J. Commun. Syst. 37 (15) (2024) e5886.

[96] T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEe Access. 6 (2018) 32979–33001.

[97] T.T.A. Dinh, et al., Blockbench: A framework for analyzing private blockchains, in: Proceedings of the 2017 ACM international conference on management of data, 2017.

[98] T. Salman, et al., Security services using blockchains: A state of the art survey, IEEE Commun. Surv. Tutor. 21 (1) (2018) 858–880.

[99] K. Salah, et al., Blockchain for AI: review and open research challenges, IEEe Access. 7 (2019) 10127–10149.

[100] N. Waheed, et al., Security and privacy in IoT using machine learning and blockchain: threats and countermeasures, ACM Comput. Surv. (csur) 53 (6) (2020) 1–37.

[101] A. Jahid, M.H. Alsharif, T.J. Hall, The convergence of blockchain, IoT and 6G: potential, opportunities, challenges and research roadmap, J. Netw. Comput. Appl. 217 (2023) 103677.

[102] H.F. Atlam, et al., A review of blockchain in Internet of things and AI, Big. Data Cogn. Comput. 4 (4) (2020) 28.

[103] H. Luo, et al., Convergence of symbiotic communications and blockchain for sustainable and trustworthy 6G wireless networks, IEEe Wirel. Commun. 32 (2) (2025) 18–25.

[104] A. Sharma, S. Kaur, M. Singh, A comprehensive review on blockchain and Internet of Things in healthcare, Trans. Emerg. Telecommun. Technol. 32 (10) (2021) e4333.

[105] N.K. Trivedi, et al., Impact analysis of integrating AI, IoT, big data, and blockchain technologies: A comprehensive study, in: 2023 3rd Asian Conference on Innovation in Technology (ASIANCON), IEEE, 2023.

[106] A. Heidari, et al., Securing and optimizing IoT offloading with blockchain and deep reinforcement learning in multi-user environments, Wireless Netw. 31 (4) (2025) 3255–3276.

[107] M.A. Ferrag, et al., Blockchain technologies for the internet of things: research issues and challenges, IEEe Internet. Things. J. 6 (2) (2018) 2188–2204.

[108] W. Liang, N. Ji, Privacy challenges of IoT-based blockchain: a systematic review, Cluster. Comput. 25 (3) (2022) 2203–2221.

[109] F. Xu, H.-C. Yang, M.-S. Alouini, Energy consumption minimization for data collection from wirelessly-powered IoT sensors: session-specific optimal design with DRL, IEEe Sens. J. 22 (20) (2022) 19886–19896.