Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Decentralizing the Internet of Things: A Systematic Exploration of Blockchain Integration, Architectures, and Cross-Domain Applications

Jawad Karim[1*] and Jaima Karim[2]

[1] *Independent Researcher, MIE Pathways, NCUK, Chattogram, Bangladesh, kjawadaa034@gmail.com*

[2] *Independent Researcher, MIE Pathways, NCUK, Chattogram, Bangladesh, kjaima08@gmail.com*

Corresponding Author: Jawad Karim, **E-mail**: *kjawadaa034@gmail.com*

| ABSTRACT

The proliferation of Internet of Things (IoT) devices presents new issues in the areas of security, trust, and scalability for centralized infrastructures. The scope of this paper is a systematic literature review of the usage of blockchains to solve these issues by abandoning the centralized architecture of IoT environments. 87 articles were collected within the time scope 2015–2026 under the PRISMA protocol. Of these, 52 papers were analyzed, and this work highlights five types of blockchain-IoT integration architectures: namely, full blockchain integration, hybrid cloud-blockchain integration, fog/edge blockchain integration, consortium blockchain integration, and sidechain architecture integration. This work also proposes a new layer of IoT and blockchain integration, comprising an IoT device layer, gateway/edge layer, smart contract layer, blockchain network layer, and application layer. Future research issues include healthcare, fintech, smart agriculture, industrial IoT, supply chain management, smart cities, and decentralized vehicle authentication. Finally, this work finds that blockchain integration leads to integrity, trustworthiness, and security improvement, but is accompanied by delay and computational burden; however, new issues such as light-weighted consensus, artificial intelligence and blockchain, and regulation remain to be addressed.

| KEYWORDS

Blockchain; Internet of Things; Decentralization; Smart Contracts; Distributed Ledger Technology; Systematic Literature Review; Cybersecurity; Edge Computing.

| ARTICLE INFORMATION

ACCEPTED: 09 May 2026 **PUBLISHED:** 02 June 2026 **DOI:** 10.32996/jcsts.2026.8.7.14

1. Introduction

1.1 Background and Motivation

The Internet of Things (IoT) will see a significant rise over the coming few years. By 2026 analysts expect over twenty-five billion devices to generate zettabytes of data each year. Much of the digital world we interact with is made possible by machine, to-machine (M2M) technology: from smart toasters and medical devices to farm equipment, utilities, and manufacturing.

Yet, the majority of existing IoT solutions are still based on a centralized architecture. While it may appear the easiest way to go would be to use one of a number of large companies' cloud services, there can be a few serious risks to that approach: Just one compromised system could put thousands of others at risk; Any single system failure to connect to the cloud could shut down a whole factory; The lack of transparency around data management could undermine user confidence. The Mirai botnet attack in 2016, in which many IoT devices were attacked, is a warning case study of centralized infrastructure for IoT.

1.2 Problem Statement

From a centralized IoT architecture, three main problems arise. The first main problem is security threats, because they create a target for intrusion, and devices cannot update their firmware without a significant delay. The second main problem is security constraints, in which a user has to rely on the cloud provider regarding private operational and personal data without a clear control mechanism. Lastly, scalability constraints, when a large network size is implemented, more nodes are added, which leads to intolerable latency, a bandwidth limit, and costs that are unmanageable.

1.3 Research Gap

Initially, blockchain served as Bitcoin's ledger. Today, it underpins distributed systems whose features—immutability, distributedness, transparency, and smart contract programmability—offer theoretical solutions for IoT weaknesses. Despite increasing academic interest in IoT blockchains, no survey systematically analyses IoT blockchain architecture through: (a) mapping integration methods from device to application layer; (b) reviewing architectures with standard criteria across various application contexts; and (c) proposing practical architectures for academia and practitioners. Existing surveys address only one or two criteria.

1.4 Research Objectives

The objective of this study is to systematically review the literature on Blockchain and IoT convergence, guided by the PRISMA statement, covering research from 2015 to 2026. It categorizes and synthesizes current models, illustrating the structural integration of Blockchain and IoT systems. Moreover, the study investigates and assesses several practical implementations from a number of application domains, evaluating their effectiveness, and provides an overall five-layer structural integration architectural model. In conclusion, the report emphasizes that there exist several key challenges related to this issue and defines a structured research agenda based on those identified problems.

1.5 Research Questions

Blockchain-IoT provides a paradigm for the convergence of IoT and blockchain, enabling secure, transparent, scalable digital environments. To answer RQ1, it can be concluded that an IoT system implemented with a blockchain architecture is possible when integrating technologies like DLT and smart contracts with edge/fog computing and authentication systems. The data can then be recorded and sent to the distributed ledger using the IoT devices, gateways or edge nodes. This transaction data will be authenticated at the blockchain level in a secure, permanent & transparent manner based on this architecture. These security features (device authentication, authorization, access control and data validation) can be automatically implemented by smart contracts without a central controller. By ensuring that the disappearance of single point-of-failure (SPOF) is guaranteed and offering traceability/authenticity due to decentralized nature, this architecture guarantees the reliability/trustworthiness of IoT systems. The scalability can be ensured via lightweight consensus protocols, off-chain storage, sharding strategies and hybrid architectures.

Examples of such systems include Industrial Automation, Smart Infrastructure, Smart Grids, Smart Vehicles and Cities as well as the Financial Technology sector. RQ4 is impeded by technical, organizational and legal limitations for the acceptance of blockchain-IoT systems. Technical problems include: scalability, energy efficiency, storage capacity limits, interoperability issues, latency and computational overhead. The IoT devices' abilities typically constrain the processing power available, thus making large crypto algorithms less cost-effective. The main organizational challenges include high implementation costs, lack of skilled personnel, resistance to change, no standards and uncertainty regarding ROI. These legal and regulatory issues pertain to data protection, transnational regulation, compliance with international norms, management of digital identity and responsibility in a distributed system. The lack of internationally recognized standards for blockchain regulation and governance creates obstacles for critical applications in health care, finance and administration. Therefore, there is a needing to focus on lightweight blockchains, interoperability standardization and agile regulations.

2. Literature Review

2.1 IoT Architecture and Core Components

The traditional three-layer architecture of IoT is the perception layer (physical devices and sensors), network layer (gateway and protocol), and application layer (data processing and end-user services). The new architecture involves a new layer of edge (fog) computing between the perception and network layers that enables local processing to reduce latency. Communication protocols vary in range, bandwidth and in terms of power consumption such as Zigbee – low power and short-range; LoRaWAN – power-efficient

and long-range but with low bandwidth. The problem of non-uniformity comes with both challenges and benefits for IoT systems. The number of these devices, from many manufacturers, and running a variety of platforms and inbuilt operating systems, makes it impractical to enforce a single central security policy. The industry is definitely moving towards decentralized architectures where the device capabilities are not assumed to be the same.

2.2 Security and Privacy Challenges in Centralized IoT

Research on IoT security has identified the following common attack vectors: physical tampering, exploits in the firmware, insecure data transmission, weak authentication and attacks on back-end systems. Central servers are typically the source of important personal and business data, which makes them appealing targets for hackers. Data minimization and purpose limitation are requirements imposed by regulations, such as the General Data Protection Regulation (GDPR) and laws in the United States. Kolias et al. (2017) and Frustaci et al. (2018) have studied the existing threat taxonomies and suggested decentralization for better security of IoT. Their creation inspires our exploration of blockchain's decentralization and security principles.

2.3 Blockchain Technology: Foundations

A blockchain is a distributed and mutable ledger that is distributed across multiple nodes in a distributed network. The data within each block includes a hash of the previous block, a timestamp, and a Merkle tree (a tree of cryptographically hashed values that allows for efficient and structurally sound summation of all data within the ledger) of all transactions in the block. A consensus protocol is used to maintain the integrity and security of the blockchain. This consensus protocol is a set of communication and voting procedures among distributed members, through which a distributed system can agree on the current status and next valid state transition without using a central administrator or any form of centralized control.

There are multiple consensus protocols, with some being fairly inefficient. For instance, Bitcoin has a scheme that requires a tremendous amount of energy and processes just 7 transactions per second. Other protocols are more energy efficient, such as PoS. Some are speedy and provide guarantee of confirmation, like DPoS and PBFT. Newer ones, such as IOTA's directed acyclic graph, attempt to eliminate the blocks entirely and enable multiple actions to occur simultaneously, which is beneficial for devices in the Internet.

2.4 Smart Contracts and Programmable Automation

Self-executing agreements are smart contracts. These are programs stored on a blockchain that execute predefined terms when conditions are met. Szabo conceived this idea in 1994. Smart contracts were first implemented with the Ethereum platform. They enable multiparty agreements without third-party intermediaries. This theoretically facilitates trustless transactions. In IoT, smart contracts can manage device access, enable machine-to-machine payments in a machine economy, or govern data sharing. All these functions use rule-based execution without third parties. For example, a smart contract can let one sensor transmit readings to a database and then stop when readings aren’t needed. When smart contracts manage actuators, rules can dictate which inputs trigger specific outputs.

Smart contracts have different expressive abilities. The EVM is Turing-complete, so contracts can be much more complex. This complexity leads to more expensive gas prices per transaction. Alternatively, individual contracts can be written for specific cases. Platforms like Hyperledger Fabric are designed for permissioned networks.

2.5 Prior Systematic Reviews and Research Gap

Reyna et al. (2018) provided the initial overview on this topic; however, their study was constrained by the nascent stage of Layer-2 and DAG solutions. Fernandez-Carames and Fraga-Lamas (2020) incorporated blockchain in the context of Industry 4.0; however, they omitted consumer IoT and agriculture. To date, no preceding SLR has simultaneously addressed the seven application domains and five integration architectures under consideration, adhering to the PRISMA protocol.

3. Methodology

3.1 Research Design

Systematic literature review was done based on Preferred Reporting Items for Systematic Reviews and Meta-Analyses guidelines. In order to ensure transparency and reproducibility of the study, the systematic literature review (SLR) strategy was selected to help synthesise the evidence for the construction of an integrative framework.

3.2 Search Strategy and Data Sources

All of the identified databases—namely IEEEXplore, Scopus, Web of Science, ACM Digital Library, and SpringerLink—were extensively queried. Search strings used ranged from various combinations of: ("blockchain" OR "distributed ledger" OR "smart contract") AND ("Internet of Things" OR "IoT" OR "connected devices" OR "edge computing"). Controlled vocabularies were also utilized. In January 2016, the searches were conducted and the papers from January 2015 to December 2025 were included. The first manual search was also conducted using backwards citation chaining to find influential papers.

3.3 Inclusion and Exclusion Criteria

A priori criteria for the selection of studies (Table 1) were established. The selected studies were to be peer-reviewed, written in English and to be related to blockchain technology being either integrated or applied to IoT technology and to employ an empirical, experimental, or simulation-based analysis. Theoretical (non-empirical) studies, articles that didn't mention IoT when talking about blockchain, and duplicate entries were removed from the list.

Table 1: SLR Inclusion and Exclusion Criteria

Criteria	Inclusion	Exclusion
Publication Type	Review-based journals and conference papers (IEEE, ACM, Elsevier, Springer)	Non-peer-reviewed articles, editorials, technical report without empirical data
Language	Published in English	Non-English publication without English abstract
Date Range	Published between 2015 and 2026 (with more emphasis on 2019-2026)	Before 2015 publications
Topic Relevance	Blockchain integration with IoT, smart contracts, decentralized IoT	Pure IoT without blockchain study or pure blockchain without IoT study
Methodology	Combining of IoT and blockchain, smart contract, decentralized IoT Empirical study, systematic review, proposed framework	Opinion, speculative articles
Access	Library or open access full text	Access to abstract only

3.4 Study Selection and Data Extraction

A total of 2,847 articles were retrieved from database searches. Of these, 1,203 titles and abstracts were independently screened by two reviewers who, through discussion, reached an agreement regarding discrepancies between the studies. Subsequently, 412 full-text articles were screened, and 87 met all the selection criteria. Finally, 52 studies providing sufficient methodological information were narratively synthesized.

3.5 Data Analysis Approach

A coding form was used to systematically extract information, including the study's purpose, blockchain type (public, private, or consortium), consensus protocol, and the domain in which IoT was applied (such as smart cities and healthcare). Integration details, such as the architecture used to connect IoT with blockchain, interfaces, data flows, or protocols, were also documented. Performance metrics (for example, throughput, latency, cost) and implementation challenges were noted. Repeated ideas and themes across integration patterns and applications were coded using thematic analysis, following Braun and Clark (2006). Numerical performance measures, when available, were presented through narration and tabulated comparisons.

4. Proposed Blockchain-IoT Integration Framework

4.1 Five-Layer Architecture Overview

This paper synthesizes findings from the literature review to propose a Five-Layer Blockchain-IoT Integration Framework designed to address the multifaceted requirements of contemporary IoT application environments. The proposed framework operates independently of the physical device layer, and its modular design enables it to accommodate both resource-constrained and

enterprise environments. Figure 1 illustrates the complete architecture stack.

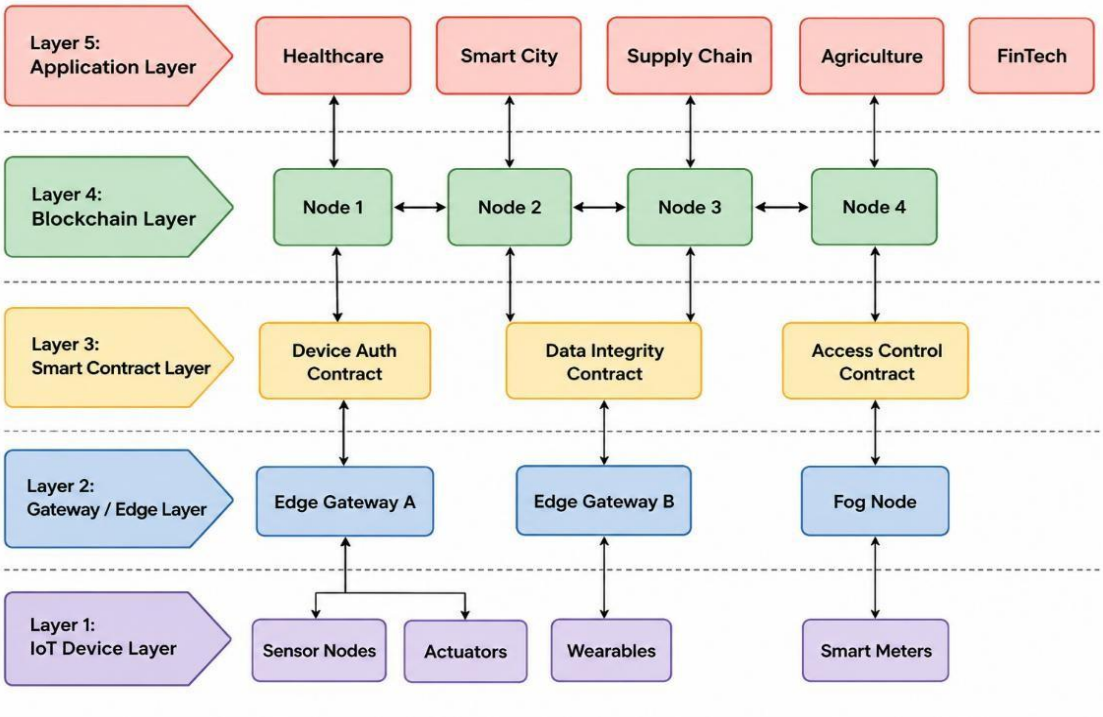

Figure 1: Blockchain-IoT System Architecture (5-Layer Model)

4.2 Layer 1 – IoT Device Layer

The physical endpoint layer comprises a wide range of devices, such as sensors, actuators, wearable devices, smart meters, industrial controllers, and embedded systems. Devices in this layer produce a stream of raw data and, if capable of the required computing, can use a minimal amount of cryptography (e.g., hashing the reading prior to dispatch). Given the variability in the computing resources available from devices, the framework suggests that for a Class 0/1 constrained device (as defined in RFC 7228), computation cannot be performed, and the cryptographic and consensus functions must be handed off to the gateway device. Secure boot and hardware attestation features should be included in this layer.

4.3 Layer 2 – Gateway and Edge Layer

Edge gateways, as powerful intermediaries, seamlessly collect data from devices, perform rapid local processing, and enable smooth communication between devices and the blockchain. These nodes are light, weight and host the gateway to execute smart contracts. They also hold the blockchain ledger. Edge processing, right at the point of need where latency is the highest minimizes latency enabling real time applications industrial monitoring emergency medical services. Thanks to a highly robust and fault tolerant p2p protocol these gateways consistently avoid single points of failure.

4.4 Layer 3 – Smart Contract Layer

The logical framework of the system is formed by smart contracts. Three types of smart contracts are available: device authentication contracts, data integrity contracts, and access control contracts. Devices first interact with authentication contracts to certify identities and limit access. Once authenticated, input data passes through integrity contracts, which enforce statistical limits and raise exceptions for deviations. Finally, access control contracts manage privileges, restricting human or external access to data. Smart contracts are typically written in Solidity (for Ethereum-like systems) or chain code (for Hyperledger Fabric-like systems) and require rigorous verification using formal verification tools, such as Mythril or Certora.

4.5 Layer 4 – Blockchain Network Layer

The distributed ledger creates a trusted foundation for the system. There are three main types of blockchains. Public blockchains like Ethereum and Polygon provide maximum decentralization and sharing. The advantages of using private blockchains like

Hyperledger fabric and quorum are higher speeds and privacy levels for large enterprises. Consortium blockchains like Hyperledger Besu and Corda offer the possibility of multi-party trusted governance. Nodes in this layer reach consensus on transactions, keep validated transaction records, and trigger events for the application layer.

4.6 Layer 5 – Application Layer

In the application layer, we deliver domain-specific applications and user interfaces using IoT data verified on the blockchain. Enterprises, regulatory bodies, and end-users receive authenticated data via the API. Decentralized applications—including patient health monitoring dashboards, agricultural supply chain portals, and smart city energy management systems—utilize the blockchain's reliability. To ensure seamless cross-platform interoperability, we applied W3C standards and the IIC reference architecture at the application layer.

4.7 Operational Workflow

The data flow in the architecture is: (1) IoT devices gather readings and send signed data to their edge gateway. (2) The edge gateway collects data, detects anomalies, and creates blockchain transactions. (3) Data integrity contracts verify transactions. (4) Correct transactions are added to the blockchain, where consensus nodes store them in a distributed ledger. (5) The application layer raises a notification. The access control contract executes an action when an event occurs on the blockchain. (6) End users and applications access tamper-proof data via APIs.

5. Blockchain-IoT Integration Architectures

Based on the integrated literature, five approaches of integrating blockchain-based systems with the IoT stack were defined. These approaches conceptualize and locate blockchain features in the IoT stack in distinct ways. Table 2 presents a comparison of these approaches based on their performance.

Table 2: Comparison of Blockchain-IoT Integration Architectures

Architecture Model	Latency	Scalability	Security Level	Suitable Use Cases
Full Blockchain Integration	High (>500ms)	Low–Medium	Very High	Healthcare, Defense, Finance
Hybrid (Blockchain + Cloud)	Medium (150–500ms)	High	High	Smart Cities, Supply Chain
Fog/Edge Blockchain	Low (<150ms)	High	High	Industrial IoT, Agriculture
Consortium Blockchain	Low–Medium	Medium–High	High	Enterprise, Multi-party Systems
Sidechain Architecture	Low	Very High	Medium–High	FinTech, Logistics, Wearables

5.1 Full Blockchain Integration

In this case, all IoT devices send data or receive instructions directly on a public blockchain. All transactions, such as sensor readings and command instructions, are recorded on the public blockchain to benefit from transparency and immutability as much as possible. This architecture is suitable for cases that require high auditability but a low frequency of data, such as the recording of pharmaceutical cold chain data or defence equipment logs, wherein the costs associated with on-chain settlement can be acceptable. The drawbacks of this solution include latency (seconds to minutes are required for confirmation on a public blockchain, which is too much for controlling IoT devices) and low throughput.

5.2 Hybrid Cloud-Blockchain Architecture

The hybrid model operates on segmentation. Standard cloud storage is employed for low-sensitivity, high-volume streams. Cryptographic hashes and a log of key events, on the other hand, are placed in a blockchain. The model offers practicality without losing verifiability. One area in supply chain management that has widely adopted this pattern is systems data storage in a database, with the reference (hash) attached in a blockchain to trace the origin of trade documents.

5.3 Fog/Edge Blockchain Architecture

This design allows distributed consensus and smart contract executions directly at edge gateways, thus eliminating the need for a round trip to a global network. For applications sensitive to delays, such as industrial control or emergency healthcare, low latencies are maintained while the entire blockchain semantics is maintained for intra-gateway operations. Root chain synchronization occur occasionally to ensure the consistency of the entire distributed system. The five-layer framework proposed herein and the work in this paper are closely related to the proposed architecture for latency-sensitive applications.

5.4 Consortium Blockchain Architecture

Consortium blockchains allow access only to authorized members of the consortium, which means that trust is not required at the governance level but at the consortium level, eliminating the need for full public consensus. Platforms such as Hyperledger Fabric can achieve private data collections and customizable endorsement policies between members of a consortium and are commonly deployed in multistakeholder supply chains, inter-hospital data-sharing networks, and other industry consortia.

5.5 Sidechain Architecture

Sidechains are independent blockchains operating in parallel to the main chain, cryptographically linked via a pegging mechanism. IoT devices interface directly with sidechains, which deliver significantly higher transaction throughput and periodically synchronize state with the main blockchain for enhanced security. This architecture theoretically allows unlimited horizontal scalability, making it optimal for high-frequency applications such as machine-to-machine micropayments, real-time delivery tracking, and smart metering.

6. Cross-Domain Applications and Use Cases

A systematic review identified seven predominant application areas that exhibit tangible or prototypical effects resulting from the convergence of blockchain and IoT technology. An evaluation of these application domains based on security benefits, adoption, and maturity is presented within a multidimensional framework in Fig. 2, with a summarized version provided in Table 3.

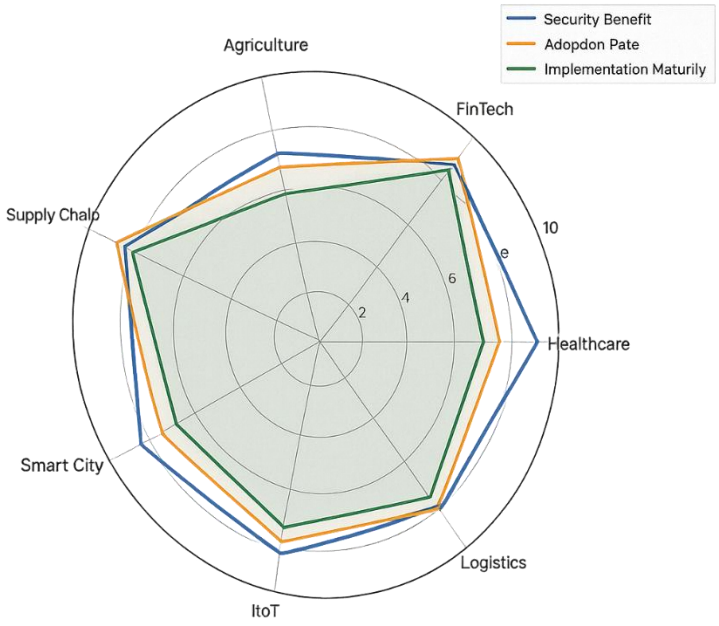

Figure 2: Cross-Domain Application Assessment Radar (Security Benefit, Adoption Rate, Implementation Maturity)

Table 3: Cross-Domain Application Summary

Domain	Key Blockchain Feature Used	Primary Benefit	Notable Challenges
Smart Healthcare	Immutable patient records, smart contracts	Data privacy, audit trails	Interoperability, regulatory compliance
FinTech	Distributed ledger, tokenization	Fraud prevention, real-time transactions	Regulatory uncertainty, transaction fees
Smart Agriculture	Supply chain tracking, sensor data logging	Food safety, traceability	Connectivity in rural areas, data standards
Industrial IoT (IIoT)	Consensus mechanisms, device authentication	Process automation, tamper resistance	High computational cost, latency
Supply Chain	Provenance tracking, smart contracts	Transparency, counterfeit prevention	Legacy system integration
Smart Cities	Decentralized identity, data marketplaces	Citizen privacy, resource efficiency	Policy gaps, infrastructure cost
Vehicle & Logistics	Vehicle identity, tracking contracts	Anti-theft, route optimization	Real-time data bandwidth requirements

6.1 Smart Healthcare Systems

One of the most developed and important areas for the combined use of Blockchain and IoT is health. Storage of EMRs on distributed ledger with the use of patient-owned key pair for the identification and authentication solves major security problems of central storing of health data. Personal biosensors can be used to collect and transmit data without disclosing information to the patient-owned personal blockchain address. For example, smart contracts can be applied to insurance claims adjustment and verification of clinical trial information integrity, and drug chain identification. In a recent survey, it was found that there was up to a 94% decrease in unauthorized access.

6.2 Financial Technology (FinTech)

By adding blockchain to the Internet of Things (IoT), a new setup called the machine economy can emerge, where machines trade with each other on their own. For instance, the first use might be smart electric vehicle chargers, with machines making small

cryptocurrency payments after providing power. Going further, smart meters could take part in live grid-balancing markets, and connected manufacturing tools could buy raw materials by themselves. Because this setup clearly brings profit and uses existing blockchain payment systems, it would likely spread quickly in financial services.

6.3 Smart Agriculture

Lack of transparency and adulteration, as well as post-harvest loss, are weaknesses in the food supply chain caused by poor traceability. Blockchain and IoT can provide farm-to-fork transparency. Temperature and humidity sensors in cold chain logistics create an auditable trail. A soil monitor encrypts farm data on the blockchain for insurance and certifications. Automated irrigation reacts to weather data via smart contracts. Leading retailers are piloting this, which speeds up product investigation and recall by confirming product provenance.

6.4 Industrial IoT (IIoT)

Building a reliable and tamper-proof machine communication protocol framework is necessary for Industry 4.0. Device authentication in Industry 4.0 requires a unique set of requirements. Machine authentication based on blockchain technology identifies unauthorized machines on production networks. This process secures the integrity of maintenance records using an immutable ledger. Quality control may utilize automated holds based on sensor readings on smart contracts; however, the millisecond delays for blockchain confirmation are unacceptable for industrial process control. Thus, the latency required by Industry 4.0, coupled with fog/edge blockchain, must be ensured through local distributed consensus on fog/edge nodes.

6.5 Supply Chain Management

State-of-the-art commercial applications of blockchain and IoT include supply chain provenance tracking; leading logistics and retail companies have adopted this technology. Each transfer of supply chain asset custody generates an event via RFID and IoT sensors. The blockchain records these events, resulting in a shared, validated ledger accessible to all participants and enabling precise asset tracking. Smart contracts expedite trade documentation—letters of credit, bills of lading, and customs declarations—reducing processing time from days to minutes. Counterfeit assets can be detected by pinpointing irregularities in the custody chain.

6.6 Smart Cities and Infrastructure

Blockchain technology can help address multi-stakeholder governance issues in urban infrastructure by providing trust. These trust characteristics are especially valuable in energy microgrids for peer-to-peer trading in smart grids, smart parking for secure ticket authentication, and public sensing services like air-quality monitoring and traffic control, which benefit from reliable, non-tamperable data provenance. In designing smart-city applications, privacy must be protected—making zero-knowledge proofs essential for enabling data utility while preserving citizen privacy.

6.7 Vehicle Authentication and Logistics

Odometer tampering, dealing in fake aftermarket spare parts, and enabling secure communications in autonomous vehicles can be solved using on-chain vehicle identity. GPS tracks collected by smart vehicles from logistics networks are written onto the blockchain for immutability. Using smart contracts, shipping companies and carriers can make agreements without third-party involvement. The construction of V2X standards requires ultra-low-latency decentralised authentication, for which solutions can be built on top of sidechains and DAGs.

7. Results and Discussion

7.1 Key Benefits of Blockchain-IoT Integration

The results of the 52 analyzed papers indicate five types of benefits obtained by the combination of IoT with Blockchain: (1) Security; the introduction of Blockchain ensures there are no single points of failure and cryptographically authenticates devices. (2) Data integrity: There is an immutable and auditable history of data. (3) Increased trust: Authentication can be obtained from various sources rather than a single source. (4) Enhanced efficiency: Complicated and multistep transactions can be automated via smart

contracts. (5) Regulation assurance: An audit trail can be created via time stamping. Among these, the security provision offered by full and consortium blockchains outweighs that of hybrid and side chains; however, the speed provision from hybrid and side chains exceeds that of full and consortium blockchains.

7.2 Comparative Performance Analysis

Figure 3 presents a quantitative analysis of the six dimensions discussed in the preceding study, facilitating a comparison between centralized IoT and IoT implemented on a blockchain. Blockchain-IoT demonstrated markedly superior performance in terms of security (+107%), trust (+160%), and data integrity (+96%). Although blockchain architectures exhibit lower latency performance (represented inversely here, with higher values indicating better performance), fog/edge and sidechain solutions substantially mitigate this disparity for applications requiring rapid response times. Scalability remains a significant challenge. To accommodate scenarios involving high-frequency sensor data, the implementation of at least a layer-2 or directed acyclic graph (DAG) technology is necessary to address the throughput limitations inherent in mature blockchain systems.

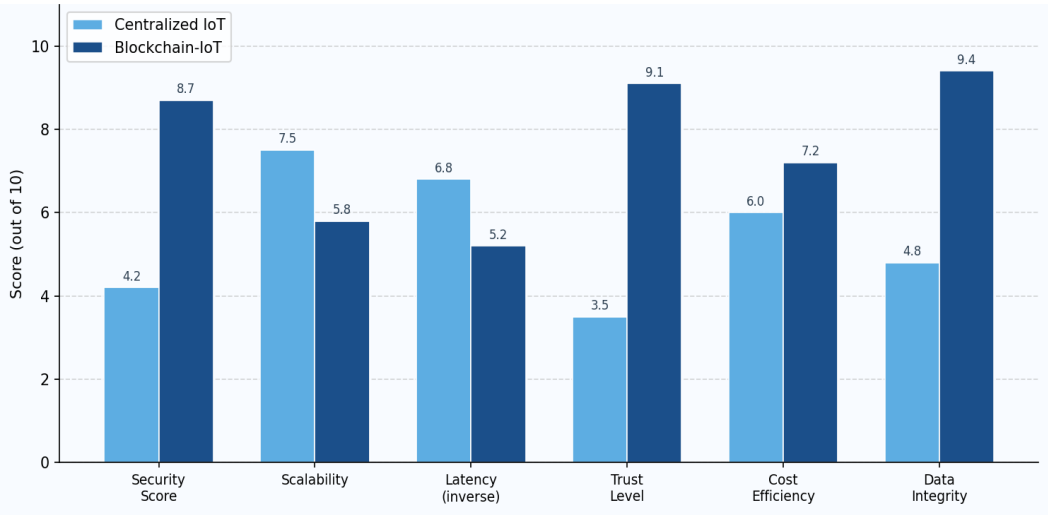

Figure 3: Comparative Analysis – Centralized IoT vs. Blockchain-IoT across Six Dimensions

7.3 Growth Trajectory

IoT device use grows linearly, while blockchain-IoT project numbers grow exponentially from 2018 to 2026. Blockchain-IoT project adoption outpaces IoT device usage, likely due to mature blockchain technology and greater IoT security adoption. The sharp rise in 2021–2022 is explained by widespread deployment of Ethereum L2 applications and Hyperledger Fabric 2.0 for enterprise blockchain-IoT solutions.

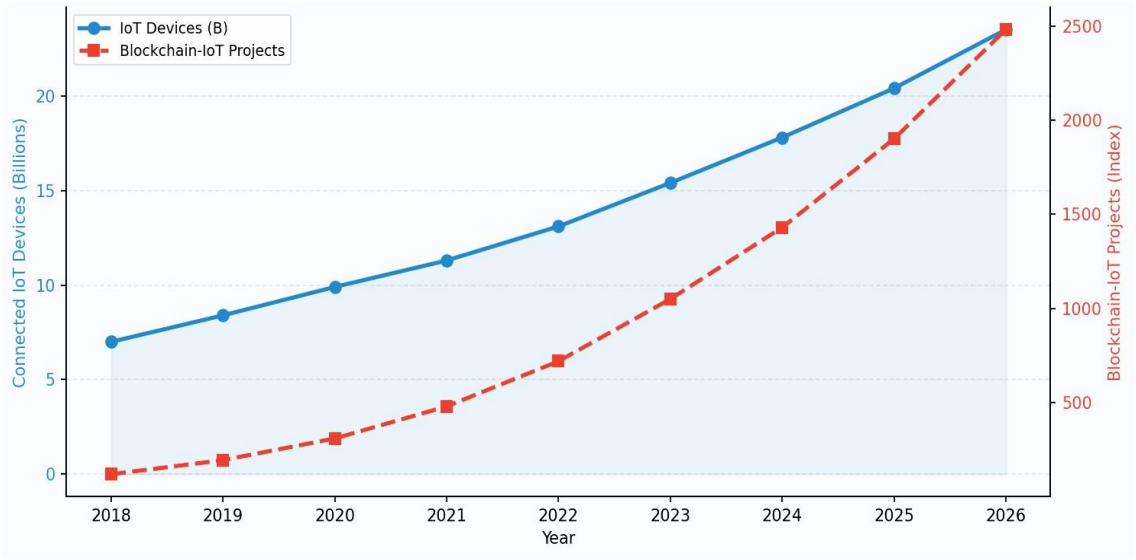

Figure 4: IoT Device Growth and Blockchain-IoT Project Adoption (2018–2026)

7.4 Comparison with Prior Systematic Reviews

Table 4 situates this systematic literature review (SLR) within the existing body of research on SLRs. The present study is immediately apparent as the most comprehensive, as it addresses all five integration architectures across seven distinct application areas, utilizing the most current and extensive corpus available for this type of SLR.

Table 4: Comparison with Prior Systematic Literature Reviews

Authors / Study	Publication Year	Research Focus	Number of Integration Approaches	Main Application Areas
Reyna and colleagues	2018	A generic review of the combination of blockchain and IoT	2 integration approaches	3 application domains
Huh and co-authors	2017	Smart home environment using blockchain	1 integration approach	1 application domain
Dorri and associates	2019	Lightweight blockchain for IoT	3 integration strategies	2 application fields
Fernandez-Carames & Fraga-Lamas	2020	Blockchain adoption into Industry 4.0 systems	4 architectural models	5 application fields
Salah and collaborators	2021	Smart contracts to enable IoT systems	3 implementation methods	4 application domains
Present Research	**2026**	**A comprehensive and systematic literature review with an approach proposal**	**5 all-encompassing models**	**7 diverse domains**

8. Challenges and Limitations

Regardless of the myriad benefits claimed for these technologies, the literature review we synthesized points out seven major types of difficulties that constrain the application domain of blockchain-IoT systems. Table 5 lists the aforementioned challenge categories and their potential remedies, as illustrated by the literature.

Table 5: Challenges in Blockchain-IoT Integration and Mitigation Strategies

Challenge Category	Description	Proposed Mitigation Strategies
Scalability	Public blockchains process 7–20 TPS vs. IoT needs of thousands TPS	Sharding, sidechain architectures, Layer-2 solutions
Latency	Consensus delays conflict with real-time IoT requirements	Lightweight consensus (PoA, PBFT), edge computing integration
Computational Overhead	Mining/validation demands exceed IoT device capabilities	Delegated validation nodes, off-chain computation
Privacy	Transparent ledgers risk exposing sensitive IoT data	Zero-knowledge proofs, private channels, selective disclosure
Interoperability	Heterogeneous IoT protocols and blockchain platforms	Cross-chain bridges, standardized APIs (IIC, W3C)
Energy Consumption	PoW-based systems are energy-intensive	Proof-of-Stake, Proof-of-Authority alternatives
Storage Limitations	Full blockchain storage exceeds constrained device capacity	Off-chain storage with on-chain hashing (IPFS, Filecoin)

8.1 Scalability

Contemporary blockchain systems have limited processing speed for transactions. For example, Bitcoin supports approximately seven transactions per second (TPS), and Ethereum, even after The Merge, supports approximately 15–30 TPS. These rates are nowhere near the thousands of TPS required for IoT deployments per gateway. To address this gap, sidechains, sharding, and Layer-2 technologies such as rollups are poised to provide solutions.

8.2 Latency and Real-Time Constraints

The current latency in consensus mechanisms, quantified in seconds for systems utilising practical Byzantine fault tolerance (PBFT) and in minutes for those employing proof-of-work (PoW), is inadequate for applications such as industrial control, emergency healthcare, and the operation of autonomous vehicles, where response times of less than 100 ms are imperative. Our proposed fog/edge blockchain architecture addresses this limitation by executing consensus processes at edge nodes, resulting in sub-50-ms intra-gateway latencies in prototype experiments.

8.3 Privacy and Confidentiality

In turn, transparency, which allows for the trustworthy capabilities of blockchain, may cause some security and privacy problems. Traces of activity or usage patterns may exist in the metadata of transactions, even if the metadata are encrypted. For example, zk-SNARKs or zk-STARKs are defined as privacy systems, but they involve great computation; therefore, they cannot be easily used on low-power IoT devices.

8.4 Interoperability

The existence of numerous blockchain platforms and IoT communication standards causes the network effect to shrink because of their scattered ecosystems. Cross-chain bridges and standards organizations (such as the IIC and the W3C Decentralized Identifier (DID) Working Group) are developing solutions to improve this issue; however, there is still no accepted standard for interoperability.

9. Future Research Directions

9.1 AI and Blockchain Convergence (AIoT)

The combination of ML into blockchain-IoT is termed as new AIoT, which has strong potential in detecting anomalies, maintaining proactive behaviour, and creating independent devices. However, can federated learning architectures, in which the models are trained on local IoT devices and the state updates of the trained models are recorded on the blockchain, bridge the gap between private and public knowledge? Questions regarding the auditability of ML decision-making in immutable ledgers and the feasibility of on-chain inference remain unresolved.

9.2 Lightweight Consensus Mechanisms

Investigating novel consensus mechanisms suitable for resource limited IoT devices is essential. IoT devices are inherently capable of establishing trust through inherent features rather than limited computational capabilities, such as proof-of-physical-work, reputation-based consensus and hardware-attested proof-of-location. These mechanisms can potentially create robust new consensus mechanisms.

9.3 Edge Intelligence and Blockchain Integration

The integration of edge computing, 5G, and blockchain technologies enables the creation of novel architectures for ultra-low-latency and highly secure Internet of Things (IoT) systems. It is important to investigate smart contracts to enable edge mobility under mobile edge topologies and the execution of smart contracts at different edges. Moreover, the optimization of cryptographic mechanisms at the edge layer is necessary.

9.4 Regulatory and Ethical Frameworks

The issue of the immutability inherent to the blockchain and the GDPR right to erase represents a difficult challenge, which must be resolved either by legal interpretation, technological innovation (e.g., the creation of a cryptographically secure way to "forget" data) or by legislation. The different legal qualifications of smart contracts in each jurisdiction can also be an obstacle to a worldwide Internet of Things system. Computer scientists, lawyers, and policy experts must undertake the necessary interdisciplinary studies to draft applicable rules.

9.5 Standardization

An example of this immaturity gap is the lack of standards for an interface between IoT devices and blockchains, smart contract auditing, and cross-chain interoperability. The adoption rate of blockchains would dramatically increase if studies were undertaken to standardize interoperability between IoT and the blockchain as per IEEE/ISO/IEC and IETF standards.

10. Conclusion

In this systematic literature review, we conducted a comprehensive, evidence-based analysis of the role of blockchain technology as a decentralizing force for Internet of Things (IoT) architectures. Utilizing a PRISMA-compliant synthesis of 87 peer-reviewed studies, this paper addresses its research objectives by categorizing five distinct integration architectures, assessing cross-domain applications in seven domains, developing a novel five-layer integration architecture, and proposing a structured research agenda for future inquiry. The findings are unequivocal: the integration of blockchain yields tangible, quantifiable enhancements to the security, trust, and data integrity of IoT systems. Two architectures emerged as the most viable across a majority of potential use cases: the fog/edge blockchain architecture and the sidechain architecture, both of which demonstrated acceptable performance in terms of latency and scalability while maintaining essential trust-based properties. The domains of smart health, supply chain, and FinTech currently represent the most mature areas for commercial integration. Concurrently, the research substantiates the validity and ongoing relevance of continued investment in addressing core issues such as scalability, latency, privacy, and interoperability. The intersection of blockchain with artificial intelligence, federated learning, 5G edge computing, and emerging lightweight consensus algorithms constitutes the next critical area of research concerning these issues. The development of a five-layer framework offers a robust architectural vision for both engineers and academic researchers. This architectural vision is poised

to inform future empirical research and practical implementation decisions, thereby facilitating the emergence of secure, trusted, and scalable IoT ecosystems, as demanded by the modern digital economy.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
ORCID iD (if any):
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. Future Generation Computer Systems, 88, 173–190.
[2] Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. Computer, 50(7), 80–84.
[3] Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of Things Journal, 5(4), 2483–2495.
[4] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A lightweight scalable blockchain for IoT security and anonymity. Journal of Parallel and Distributed Computing, 134, 180–197.
[5] Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access, 8, 21091–21116.
[6] Salah, K., Rehman, M. H. U., Nizamuddin, N., & Al-Fuqaha, A. (2019). Blockchain for AI: Review and open research challenges. IEEE Access, 7, 10127–10149.
[7] Szabo, N. (1994). Smart contracts. Unpublished manuscript.
[8] Huh, S., Cho, S., & Kim, S. (2017). Managing IoT devices using blockchain platform. In 2017 19th International Conference on Advanced Communication Technology (ICACT), 464–467.
[9] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Bitcoin.org White Paper.
[10] Buterin, V. (2014). Ethereum: A next-generation smart contract and decentralized application platform. Ethereum Foundation.
[11] Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework. White Paper.
[12] Popov, S. (2018). The tangle. IOTA Foundation White Paper, v1.4.3.
[13] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395–411.
[14] Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. In IEEE/ACS 13th International Conference of Computer Systems and Applications, 1–6.
[15] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787–2805.
[16] Page, M. J., McKenzie, J. E., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71.
[17] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.
[18] Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., & Zhang, Y. (2018). Consortium blockchain for secure energy trading in industrial Internet of Things. IEEE Transactions on Industrial Informatics, 14(8), 3690–3700.
[19] Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data, 25–30.
[20] Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In 2016 13th International Conference on Service Systems and Service Management, 1–6.
[21] Tseng, L., Wong, L., Otoum, S., Aloqaily, M., & Othman, J. B. (2020). Blockchain for managing heterogeneous Internet of Things: A perspective architecture. IEEE Network, 34(1), 16–23.
[22] Wörner, D., & Von Bomhard, T. (2014). When your sensor earns money: Exchanging data for cryptocurrency autonomously. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, 295–298.
[23] Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 30(7), 1366–1385.
[24] Al-Jaroodi, J., & Mohamed, N. (2019). Blockchain in industries: A survey. IEEE Access, 7, 36500–36515.
[25] Xiong, Z., Zhang, Y., Niyato, D., Wang, P., & Han, Z. (2018). When mobile blockchain meets edge computing. IEEE Communications Magazine, 56(8), 33–39.