International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

A Review of Blockchain-Enabled IOT Frameworks for Secure Supply Chain and Logistics Monitoring

Vaishnav S. Swami[1], Sanjeev S. Pathak[2], Omkar S. Poojary[3], Pranjal K. Patil[4]
Mrs. Shilpa Katre[5]

[1234]Students, Department of Electronics and Computer Science Engineering,
St. John College of Engineering and Management, Palghar, Maharashtra, India
[5]Assistant Professor & Project Advisor,
Department of Electronics & Computer Science Engineering,
St. John College of Engineering and Management, Palghar, Maharashtra, India

---

Abstract - The rapid growth of global supply chains has increased the demand for secure, transparent, and reliable monitoring mechanisms, particularly for sensitive goods such as pharmaceuticals, food products, and hazardous materials. Traditional supply chain management systems rely heavily on centralized architectures, which suffer from limitations including data tampering, lack of traceability, single points of failure, and limited trust among stakeholders. In recent years, the integration of Internet of Things (IoT) technologies with blockchain has emerged as a promising solution to address these challenges.

This paper presents a comprehensive review of blockchain-enabled IoT frameworks proposed for secure supply chain and logistics monitoring. Existing literature is systematically analysed to examine how IoT-based sensing, cloud and edge computing, and blockchain-based authorization mechanisms are combined to improve transparency, integrity, and accountability across logistics operations. The review highlights commonly adopted architectural models, security strategies, and data management approaches, while also identifying key challenges such as scalability, latency, resource constraints, and real-world deployment feasibility.

Furthermore, this study compares existing solutions based on their technological focus, application domains, and limitations. The review concludes by outlining open research gaps and future directions, emphasizing the need for lightweight, scalable, and practical frameworks capable of supporting large-scale logistics ecosystems.

***Key Words*:** *Internet of Things, Blockchain, Supply Chain Monitoring, Secure Logistics, Cloud Computing, Traceability, Cyber-Physical Systems.*

I. INTRODUCTION

Global supply chains have evolved into complex, geographically distributed ecosystems involving manufacturers, logistics providers, regulators, distributors, and end consumers. The growing movement of temperature-sensitive, high-value, and compliance-critical goods such as pharmaceuticals, perishable food products, and chemical materials has significantly increased the demand for reliable monitoring and traceability mechanisms [14]. Traditional supply chain infrastructures were primarily designed around centralized enterprise management systems, which often lack transparency and real-time data synchronization across stakeholders [1], [6].

The introduction of the Internet of Things (IoT) has transformed logistics monitoring by enabling continuous sensing of environmental and operational parameters such as temperature, humidity, location, and vibration [5]. These sensing capabilities enhance situational awareness and reduce dependency on manual reporting. However, despite operational improvements, most IoT-enabled monitoring systems continue to rely on centralized cloud architectures for data aggregation and control [8]. This reintroduces trust-related concerns, including single points of failure, data manipulation risks, and limited multi-party transparency [9].

Blockchain technology, initially conceptualized through Bitcoin's decentralized ledger model [12], and later extended through programmable smart contracts in Ethereum [13], offers a distributed and immutable record-keeping mechanism. Recent studies explore the

integration of blockchain with IoT systems to enhance auditability, non-repudiation, and trust across multi-stakeholder supply chains [10], [15]. Nevertheless, challenges related to scalability, latency, computational overhead, and real-world deployment remain active research areas [8], [9].

Given the rapid expansion of blockchain–IoT research in logistics applications, a structured and critical review is necessary to consolidate architectural models, evaluate integration strategies, and identify research gaps. This paper systematically reviews blockchain-enabled IoT frameworks for secure supply chain and logistics monitoring, focusing on architectural trends, security mechanisms, and future research directions.

II. OVERVIEW OF SUPPLY CHAIN MONITORING SYSTEMS

Supply chain monitoring systems are essential for ensuring visibility, control, and traceability across the movement of goods from production to final delivery. With increasing globalization and regulatory requirements, the need for accurate and trustworthy monitoring has grown significantly. Over time, these systems have evolved from manual and paper-based methods to digitally connected platforms that integrate sensing, communication, and data analytics technologies [1], [2]. Existing approaches can broadly be categorized into traditional centralized systems and modern IoT-enabled monitoring frameworks.

A. Traditional Supply Chain Monitoring Approaches

Traditional supply chain monitoring is primarily based on centralized enterprise management systems such as Enterprise Resource Planning (ERP), Warehouse Management Systems (WMS), and Transportation Management Systems (TMS) [6]. These platforms rely on periodic updates, barcode or RFID scans, and manual status entries recorded at predefined checkpoints. Although effective for inventory tracking and shipment coordination within single organizations, they lack real-time environmental sensing and cross-stakeholder data synchronization [1].

Centralized architectures introduce structural limitations. Data ownership remains confined to the organization hosting the system, limiting visibility for downstream partners and regulators [14]. Furthermore, reliance on periodic reporting delays anomaly detection, particularly in cold chain logistics where temperature deviations can compromise product integrity within short timeframes [11]. Centralized databases also present single points of failure and increased vulnerability to insider manipulation or cyberattacks [6]. These weaknesses highlight the inadequacy of purely centralized models for modern distributed supply chains.

B. IoT-Enabled Supply Chain Monitoring

The integration of IoT technologies has significantly enhanced supply chain visibility by enabling continuous environmental and operational sensing [5]. Embedded sensors deployed within containers and transport vehicles collect data such as temperature, humidity, geolocation, and shock exposure in real time. Such capabilities are especially critical in pharmaceutical and food logistics, where regulatory compliance depends on documented environmental stability [11].

Despite these operational benefits, IoT-based monitoring systems typically depend on centralized cloud infrastructures for data storage, analytics, and decision-making [8]. While cloud platforms provide scalability and remote accessibility, they do not inherently guarantee data immutability or decentralized trust [9]. Multi-stakeholder environments continue to face challenges in ensuring data authenticity, preventing unauthorized modification, and establishing shared accountability across organizational boundaries [10].

C. Limitations of Existing Monitoring Systems

A comparative assessment of traditional centralized systems and IoT-enabled frameworks reveals a recurring trade-off between operational efficiency and trust assurance. Centralized systems provide structured organizational control but lack transparency and resilience [6]. IoT-based systems improve real-time visibility but remain dependent on centralized backend services for validation and record management [8].

In both cases, ensuring tamper resistance, auditability, and non-repudiation across distributed stakeholders remains an unresolved issue [9]. The absence of a shared, verifiable ledger complicates dispute resolution, compliance auditing, and cross-border regulatory verification [15]. These limitations have driven research toward decentralized trust mechanisms, particularly blockchain-based frameworks, which aim to complement IoT sensing and cloud processing models [10].

III. IOT TECHNOLOGIES IN LOGISTICS MONITORING

The adoption of Internet of Things (IoT) technologies has significantly transformed logistics monitoring by enabling continuous, automated, and fine-grained observation of physical assets across supply chain

networks. IoT-based monitoring systems integrate sensing devices, embedded processing units, communication interfaces, and backend platforms to provide real-time visibility and operational intelligence. Existing literature consistently identifies IoT as a key enabler for improving responsiveness, reducing losses, and enhancing regulatory compliance in logistics operations [7], [8].

A. Sensing and Data Acquisition

Sensing is a foundational component of IoT-enabled logistics monitoring. Commonly used sensors include Global Positioning System (GPS) modules for location tracking, temperature and humidity sensors for cold-chain compliance, and motion or tamper-detection sensors for monitoring unauthorized handling [5], [6]. Continuous environmental sensing has been shown to significantly reduce spoilage and improve compliance, particularly in pharmaceutical and food supply chains [2].

However, several studies highlight limitations related to sensor accuracy, reliability, and long-term stability. Harsh operating conditions such as extreme temperatures, vibration, and prolonged deployments can degrade sensor performance over time [7]. These issues emphasize the need for calibration strategies, fault detection mechanisms, and data validation techniques, which remain insufficiently addressed in many existing solutions.

B. Embedded Platforms and Edge Devices

Embedded platforms serve as the computational backbone of IoT-based logistics systems. Microcontroller-based and system-on-chip architectures are widely adopted due to their low power consumption and compact integration capabilities [5]. These devices support local data aggregation and preliminary filtering before transmission to backend services.

Nevertheless, embedded devices face resource constraints in computation, memory, and energy availability. These limitations restrict the feasibility of performing complex cryptographic or blockchain-related operations directly at the device level [3]. Consequently, many studies advocate decoupling sensing from intensive processing by offloading verification and analytics tasks to edge or cloud layers [6].

C. Communication Technologies

Reliable communication is essential for mobile logistics monitoring. The literature explores cellular networks, low-power wide-area networks, and short-range protocols for IoT-based logistics systems [5]. Cellular connectivity remains a preferred option due to its extensive geographic coverage and support for asset mobility.

However, intermittent connectivity and variable latency present operational challenges in remote regions [7]. To address these limitations, researchers recommend buffering mechanisms, asynchronous transmission models, and resilient communication architectures.

D. Challenges in IoT-Based Logistics Systems

Although IoT enhances real-time visibility, it does not inherently guarantee data authenticity or tamper resistance. Centralized cloud storage models assume that sensor data remains trustworthy once transmitted, an assumption that has been critically examined in prior research [9]. IoT devices are vulnerable to firmware manipulation, physical tampering, weak authentication mechanisms, and insecure communication channels [7].

These vulnerabilities expose supply chain monitoring systems to risks such as data forgery, replay attacks, and unauthorized access. Consequently, researchers increasingly propose integrating decentralized verification mechanisms, particularly blockchain-based ledgers, to strengthen trust and auditability in IoT-driven logistics environments [10], [15].

IV. BLOCKCHAIN FOR SECURE SUPPLY CHAIN

Blockchain technology has emerged as a decentralized trust infrastructure capable of addressing core integrity and transparency limitations in supply chain monitoring systems. Unlike centralized databases, blockchain operates through distributed consensus mechanisms that ensure immutability and tamper resistance of recorded transactions [12]. The introduction of programmable smart contracts in Ethereum further extended blockchain's capabilities by enabling automated rule enforcement and decentralized authorization [13]. These characteristics make blockchain particularly relevant for multi-stakeholder supply chains where trust must be established across organizational boundaries.

In logistics applications, blockchain enables verifiable tracking of product movement, environmental events, ownership transfers, and compliance records [10]. By recording validated events in a distributed ledger, blockchain reduces dependency on central authorities and enhances non-repudiation across supply chain participants [14]. However, effective integration with IoT systems requires careful architectural considerations to

balance security, scalability, and operational performance [8].

A. Blockchain Integration Models in Logistics

Early blockchain-based supply chain proposals attempted to store comprehensive transaction records and sensor-generated data directly on-chain to maximize transparency [4]. While conceptually appealing, such approaches proved impractical due to limited transaction throughput, increased latency, and high operational overhead [9]. Public blockchain networks, in particular, face scalability constraints when processing frequent sensor updates in large logistics ecosystems.

To address these limitations, researchers increasingly advocate hybrid integration models [15]. In such architectures, blockchain is used primarily to store cryptographic hashes, metadata, and authorization records, while bulk IoT sensor data is maintained in off-chain storage systems or cloud databases [8]. This approach preserves the immutability and auditability advantages of blockchain while ensuring scalability and responsiveness.

Hybrid architectures also enable decoupling of authorization logic from real-time operational control. Smart contracts verify user permissions and generate verifiable transaction records, whereas execution-level commands are handled through cloud or edge services [10]. This layered design reduces blockchain congestion and improves practical deployability.

B. Security and Trust Benefits of Blockchain

Blockchain introduces several security benefits to supply chain monitoring systems. First, immutability ensures that once a logistics event is recorded, it cannot be retroactively modified without consensus across the network [12]. This property significantly strengthens audit trails and regulatory compliance reporting. Second, cryptographic signatures associated with transactions provide non-repudiation, enabling stakeholders to verify event origin and authenticity [13].

Furthermore, decentralized ledgers improve transparency by allowing authorized participants to access consistent records without reliance on a central database operator [14]. This is particularly valuable in cross-border supply chains involving independent entities with limited mutual trust [10].

However, blockchain does not inherently guarantee data correctness at the point of entry. If compromised IoT devices submit falsified data, the blockchain will preserve it immutably [9]. Therefore, secure device authentication, trusted data acquisition mechanisms, and layered verification frameworks remain essential complementary components [7]. Blockchain must therefore be integrated within a broader security architecture rather than treated as a standalone solution.

C. Limitations and Open Challenges

Despite its benefits, blockchain integration introduces new technical and operational challenges. Transaction confirmation latency and consensus overhead may affect time-sensitive logistics operations [8]. High-frequency sensor updates are particularly challenging for public blockchain networks due to throughput limitations [9].

Additionally, smart contract vulnerabilities and programming errors can introduce security risks if not carefully audited [13]. Governance models for permissioned blockchains also require clearly defined trust boundaries among participating stakeholders [15].

Energy consumption and interoperability between different blockchain platforms represent additional research concerns [8]. These challenges highlight the importance of selective blockchain usage within layered architectures that balance security guarantees with system efficiency.

V. CLOUD AND EDGE COMPUTTING INTEGRATION

Cloud and edge computing play a critical role in enabling scalable and responsive IoT-based supply chain monitoring systems. Cloud platforms provide centralized services for data storage, analytics, visualization, and integration with enterprise systems, making them a common backbone for logistics monitoring solutions. In blockchain-enabled architectures, cloud infrastructure often acts as an intermediary layer that aggregates IoT data, performs validation, and interfaces with blockchain networks to record trusted events.

However, reliance on cloud-only architectures can introduce latency, bandwidth overhead, and dependency on continuous connectivity. To address these limitations, edge computing has been increasingly adopted to process data closer to the source. Edge-based processing enables local filtering, event detection, and temporary storage, reducing communication load and improving system resilience under intermittent network conditions. Existing studies suggest that hybrid cloud–edge architectures offer a balanced trade-off between scalability, responsiveness, and operational reliability.

A. Role of Edge Intelligence in Logistics Monitoring

In blockchain-enabled logistics monitoring, cloud infrastructure often functions as an orchestration layer between IoT devices and blockchain networks [10]. Sensor data collected by IoT devices is transmitted to cloud servers, where it is validated, processed, and selectively anchored to blockchain ledgers through cryptographic hashing or smart contract transactions [8]. This approach reduces blockchain transaction load while preserving verifiable audit trails.

Cloud systems also facilitate identity management, access control enforcement, and integration with existing enterprise management platforms [14]. By acting as a middleware layer, the cloud enables compatibility between decentralized blockchain components and legacy supply chain software systems. Nevertheless, researchers caution that excessive reliance on cloud validation mechanisms may partially undermine the decentralization objectives of blockchain integration [9].

B. Edge Computing for Latency Reduction and Resilience

Edge computing enhances blockchain–IoT architectures by enabling localized processing and preliminary decision-making near the data source [8]. Instead of transmitting all raw sensor data to centralized servers, edge devices can perform data filtering, anomaly detection, and temporary buffering before synchronization with cloud or blockchain layers [5]. This reduces communication bandwidth usage and improves system responsiveness.

Edge-assisted architectures are particularly valuable in logistics environments characterized by intermittent connectivity and network latency variability [7]. For example, temperature violations can be detected locally and flagged immediately, even before blockchain confirmation occurs. This ensures operational continuity while maintaining eventual auditability through blockchain anchoring [15].

However, coordination among edge, cloud, and blockchain layers introduces architectural complexity. Consistency models, trust boundaries, and synchronization protocols must be carefully designed to prevent data inconsistency or unauthorized event injection [9]. Studies increasingly recommend clearly defined layered architectures where each component—device, edge, cloud, and blockchain—has a well-defined functional and trust role [10].

C. Hybrid Layered Architectural Models

Recent literature converges toward hybrid layered models that integrate IoT sensing, edge preprocessing, cloud orchestration, and blockchain-based authorization [15]. In these models:

- IoT devices perform sensing and basic preprocessing
- Edge nodes handle local validation and buffering
- Cloud platforms manage orchestration and analytics
- Blockchain ensures immutable authorization and auditing

Such separation of concerns enhances scalability, reduces blockchain congestion, and maintains real-time responsiveness [8]. Hybrid architectures also allow selective blockchain usage, ensuring that only critical events or authorization records are recorded on-chain rather than high-frequency raw sensor streams [9].

This layered design paradigm represents the most practical approach currently identified in the literature for real-world blockchain-enabled logistics monitoring deployments.

VI. SECURITY CHALLENGES AND EXISTING SOLUTIONS

Security in blockchain-enabled IoT supply chain systems must be analyzed across multiple architectural layers, including device, communication, cloud, and blockchain components. While integrating blockchain enhances immutability and auditability, it does not eliminate vulnerabilities inherent in IoT infrastructures or distributed computing environments [9]. A comprehensive security framework must therefore address threats spanning physical device compromise, network-level attacks, backend manipulation, and smart contract vulnerabilities.

Existing literature emphasizes that security in logistics monitoring is not a single-layer problem but a multi-dimensional challenge requiring layered defense strategies [7], [10]. Each architectural component introduces unique risks that must be mitigated through appropriate design mechanisms.

A. Device-Level Vulnerabilities

IoT devices deployed in logistics environments are often physically accessible and operate under resource constraints, making them vulnerable to firmware tampering, hardware manipulation, and weak authentication mechanisms [7]. Attackers may exploit unsecured debugging ports, inject malicious firmware, or spoof device identities to introduce falsified sensor data into the monitoring system.

Even in blockchain-integrated architectures, compromised IoT devices can inject incorrect data before it is immutably recorded [9]. Blockchain ensures data integrity after recording but cannot validate the correctness of data at the acquisition stage. Therefore, researchers recommend secure boot mechanisms, hardware-based identity modules, and encrypted communication channels to protect device-level integrity [7].

Trusted execution environments and secure device provisioning frameworks are increasingly proposed as foundational requirements for blockchain–IoT integration in logistics monitoring systems [15].

B. Communication-Level Threats

Logistics monitoring systems rely heavily on public communication networks, including cellular and internet-based infrastructures. These channels are susceptible to replay attacks, man-in-the-middle attacks, and message injection if not properly secured [6]. Intermittent connectivity further complicates secure session management, particularly in mobile logistics assets.

Encryption protocols such as TLS and mutual authentication schemes are widely recommended to ensure confidentiality and integrity during data transmission [7]. However, secure communication alone does not guarantee system-wide trust if backend validation mechanisms remain centralized.

Hybrid architectures address this limitation by combining encrypted communication with blockchain-based authorization verification [10]. In such designs, even if network interception occurs, unauthorized control commands cannot be executed without valid blockchain-backed signatures.

C. Blockchain-Specific Security Considerations

While blockchain enhances immutability, it introduces new classes of vulnerabilities. Smart contract programming errors, reentrancy flaws, and improper access control logic can lead to unintended behavior or exploitation [13]. Moreover, consensus mechanisms may expose networks to majority attacks or performance degradation in public blockchain settings [12].

Permissioned blockchain systems mitigate some of these risks by restricting validator participation but introduce governance challenges related to trust distribution among consortium members [15]. Additionally, transaction latency and confirmation delays may impact time-sensitive logistics operations [8].

Researchers therefore advocate secure smart contract development practices, formal verification techniques, and layered architectural separation between authorization logic and operational control [10]. Decoupling blockchain-based authorization from real-time device actuation improves both security and scalability.

D. Layered Security Frameworks

Contemporary research increasingly supports layered security models integrating:

•Secure IoT device identity and firmware validation
•Encrypted communication channels
•Cloud-based validation and monitoring
•Blockchain-backed authorization and immutable logging

Such layered approaches prevent single-point compromise and ensure that breaches at one layer do not cascade across the system [9], [14]. By distributing trust across multiple architectural boundaries, blockchain-enabled IoT systems can achieve stronger resilience against insider threats, external attacks, and data manipulation attempts.

However, the literature consistently emphasizes that achieving end-to-end security requires careful architectural coordination rather than simple blockchain adoption [8].

VII. RESEARCH GAPS AND FUTURE DIRECTIONS

Despite significant advancements in blockchain-enabled IoT frameworks for supply chain and logistics monitoring, several unresolved challenges remain. While the literature demonstrates the feasibility of integrating decentralized ledgers with distributed sensing systems, practical deployment at industrial scale continues to face technical and operational barriers [8], [15]. Addressing these limitations is essential for transitioning from experimental prototypes to production-ready logistics infrastructures.

This section identifies key research gaps emerging from the reviewed literature and outlines future research directions necessary to advance the field.

A. Scalability and Performance Constraints

One of the most frequently cited limitations in blockchain-integrated supply chain systems is scalability [8], [9]. Public blockchain networks struggle with high-frequency transaction loads, particularly when sensor data updates occur continuously across large logistics fleets. Even hybrid architectures that selectively anchor

metadata on-chain must carefully balance transaction volume against performance overhead [15].

Future research must focus on lightweight blockchain interaction models, including event batching, hash aggregation strategies, and layer-two scaling mechanisms. Permissioned blockchain frameworks tailored specifically for logistics ecosystems may also provide improved throughput and reduced latency [14]. However, governance models for such systems require further investigation to ensure fair trust distribution among stakeholders.

B. Data Authenticity at the Point of Acquisition

Blockchain guarantees immutability after data recording but does not inherently ensure the correctness of data at the source [9]. Compromised IoT devices or faulty sensors can inject incorrect data that becomes permanently stored on the ledger. This "garbage-in, immutable-out" challenge represents a fundamental limitation of blockchain-based monitoring systems.

Future frameworks must integrate secure device identity management, trusted execution environments, and hardware-rooted cryptographic authentication mechanisms [7]. Research into remote attestation techniques and edge-level anomaly detection may strengthen pre-blockchain data validation. Combining blockchain immutability with trusted sensing architectures remains an open research domain.

C. Interoperability and Standardization

Supply chains typically span multiple organizations using heterogeneous software platforms and blockchain networks. Interoperability across blockchain frameworks and compatibility with legacy enterprise systems remain major challenges [15]. Without standardized interfaces, large-scale adoption will remain fragmented.

Future research should prioritize development of interoperable protocols, standardized smart contract templates, and cross-chain communication models. Collaboration between academia, industry, and standards bodies will be essential to establish unified architectural guidelines for blockchain–IoT logistics systems [14].

D. Real-World Deployment and Validation

A recurring observation in the literature is the limited availability of long-term field deployment studies [8]. Many blockchain-enabled IoT proposals remain conceptual or validated only through small-scale simulations. Comprehensive field trials across large logistics networks are necessary to evaluate performance under real operational constraints.

Future research must emphasize empirical validation, including latency benchmarking, security stress testing, and resilience analysis under network disruption conditions. Integration with regulatory compliance frameworks and industrial auditing processes also requires deeper investigation [11], [15].

E. Energy Efficiency and Sustainability Considerations

Energy consumption associated with blockchain consensus mechanisms presents another research concern, particularly in environmentally conscious logistics operations [9]. Although permissioned blockchains reduce computational overhead compared to proof-of-work systems, sustainability trade-offs must be evaluated carefully.

Emerging research directions include energy-efficient consensus algorithms, edge-assisted blockchain participation models, and optimized cryptographic operations tailored for IoT ecosystems [8]. Sustainable blockchain design will be critical for long-term adoption in large-scale logistics networks.

Collectively, these research gaps indicate that blockchain-enabled IoT supply chain monitoring remains a rapidly evolving domain. While architectural frameworks demonstrate strong theoretical benefits in transparency and trust enhancement, practical scalability, interoperability, and device-level trust remain open research challenges [10].

VII. CONCLUSION

This review systematically examined blockchain-enabled IoT frameworks proposed for secure supply chain and logistics monitoring. The analysis demonstrates that IoT technologies significantly enhance operational visibility by enabling continuous sensing of environmental and logistical parameters, thereby improving responsiveness and compliance tracking in modern supply chains [5], [11]. However, conventional IoT-based architectures remain dependent on centralized cloud infrastructures, which introduce concerns related to trust, data manipulation, and single points of failure [8], [9].

Blockchain technology introduces decentralized immutability, non-repudiation, and verifiable audit trails, offering a promising solution to the transparency limitations of traditional monitoring systems [12], [13]. Research indicates that hybrid integration models—where blockchain is selectively used for authorization

and audit logging while bulk data remains off-chain—represent the most practical architectural approach for real-world deployment [15]. Such layered architectures effectively balance scalability, performance, and security requirements across distributed supply chain ecosystems [10], [14].

Despite these advancements, significant challenges persist. Scalability constraints, latency overhead, interoperability limitations, and the unresolved issue of data authenticity at the point of acquisition remain critical research areas [8], [9]. Furthermore, long-term industrial validation and standardized architectural guidelines are necessary to transition blockchain-enabled IoT monitoring frameworks from experimental prototypes to large-scale operational systems [15].

In conclusion, blockchain-enabled IoT integration represents a transformative direction for enhancing trust and transparency in supply chain monitoring. However, successful deployment requires carefully engineered layered architectures that integrate secure sensing, resilient communication, scalable cloud orchestration, and selective blockchain anchoring. Continued interdisciplinary research and industry collaboration will be essential to realize secure, scalable, and deployable logistics monitoring infrastructures in future global supply chains.

REFERENCES

1. Vishal Chauhan & Aarushi Chauhan, "Blockchain Technology in Supply Chain Management," International Journal of Scientific Research in Engineering and Management (IJSREM).

2. Vidhya K., Bhoomika S., Deepu Bai & Lavanya S., "Implementation of a Blockchain Based Supply Chain Management System," International Journal of Scientific Research in Engineering and Management (IJSREM), Dec. 2025.

3. Madhuri Vaghasana & Divya Suliya, "Review on Precise of Blockchain Technology," International Journal of Scientific Research in Engineering and Management (IJSREM), Mar. 2023.

4. "Blockchain-Based Supply Chain Tracking System – Implementation of a Decentralized Smart Contract on Ethereum," IJSREM, Nov. 2024.

5. Aman S. Ghani, "Revolutionizing Supply Chains: A Comprehensive Study of Industry 4.0 Technologies (IoT, Big Data, AI, etc.)," International Journal of Scientific Research in Engineering and Management (IJSREM).

6. A. B. Surkunde, R. Patil, S. Deshmukh, and P. Kulkarni, "Transforming Supply Chain Management with Big Data and IoT Innovations," *International Journal of Scientific Research in Engineering and Management (IJSREM)*, Dec. 2024.

7. National Institute of Standards and Technology, *IoT Device Cybersecurity Capability Core Baseline*, NISTIR 8259A, 2020 — provides foundational cybersecurity criteria for IoT systems integrated with backend services.

8. A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT: Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018.

9. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in internet of things: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1731–1758, 2017.

10. K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system," *IEEE Access*, vol. 5, pp. 17465–17477, 2017.

11. M. Kim and J. Park, "Blockchain-based data management for cold chain logistics," *Journal of Industrial Information Integration*, vol. 15, pp. 100–108, 2019.

12. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

13. Ethereum Foundation, "Ethereum white paper," 2014.

14. H. Min, "Blockchain technology for enhancing supply chain resilience," *International Journal of Production Research*, vol. 57, no. 7, pp. 2173–2184, 2019.

15. X. Xu, Q. Lu, Y. Liu, L. Zhu, H. Yao, and A. V. Vasilakos, "Designing blockchain-based applications: A case study for supply chain," *Future Generation Computer Systems*, vol. 92, pp. 64–77, 2019.