A Systematic Review of Deep Learning-Enabled Post-Quantum Blockchain Frameworks for Secure and Sustainable Supply Chain Management

Chetan Chauhan[1], Dr. Bharati Ainapure[2,3]
[1]Post Doctoral Research Scholar, Lincoln University College, Malaysia, India ; [2]Adjunct Research Faculty under the Lincoln Global Postdoctoral Researcher (LGPR) Programme at Lincoln University College, Malaysia; [3]Professor, Department of Computer Engineering, Vishwakarma University, Pune, India.
Email ID: [1]er.chouhan.chetan@gmail.com, [2]bharati.ainapure@vupune.ac.in

Abstract: In the interest of global supply chains becoming more data heavy, digital and more vulnerable to adversarial manipulation, blockchain, deep learning, and cryptographic security research have converged. Blockchain ledgers provide an immutable source of origin and trust to multi-party logistics networks, and deep learning models provide predictive and anomaly-detection capabilities to manage demand volatility, sensor noise, and cyber-physical risks at IoT-enabled supply chain points. The cryptographic primitives used in the consensus mechanisms and signature schemes of present-day blockchains and the one currently used in the crypto layer, however, are known to be provably vulnerable to Shor's and Grover's quantum algorithms, placing a long-term security burden on any supply chain infrastructure that relies on classical hardness assumptions. This review aims to present an overview of the twenty-two peer-reviewed and IEEE-indexed papers related to blockchain-based supply chain security, AI-enabled blockchain, federated deep learning, IoT and edge security, post-quantum cryptography (PQC), and quantum-secure blockchain architectures, in order to build a solid understanding of how these four technological layers can be integrated into a coherent supply chain security stack. The review builds a comparative analysis of blockchain frameworks, PQC algorithm families, deep learning architectures, and agriculture, healthcare, vehicular network, geospatial systems and cloud storage, among others. This synthesis is extended to an original taxonomy, which shows the technological evolution from deep learning to blockchain, post-quantum cryptography, supply chain security and sustainability and a conceptual framework composed of 9 layers, going from data collection and IoT sensing, to edge intelligence, federated deep learning, post quantum cryptographic hardening, blockchain consensus, smart contract execution, supply chain analytics and decision support.
Keywords: Post-Quantum Cryptography; Blockchain; Deep Learning; Supply Chain Management; Federated Learning; IoT Security; Quantum-Resistant Consensus; Sustainable Digital Infrastructure

Introduction

Today's supply chains are digital, interconnected, and huge, with manufacturers, suppliers, logistics, distributors, and retailers interacting and exchanging vast quantities of data across a geographically dispersed network. As the use of digital technologies such as information and communication systems has grown, it has contributed to the general efficiency of operations, inventory management, and decision making, but has also raised several new questions of security, privacy, and trust. New technologies like blockchain, artificial intelligence, the Internet of Things (IoT), cloud computing, and edge computing have revolutionized traditional supply chain workflows, making them smart, datacentric, and capable of real-time monitoring and predictive analytics. By harnessing vast amounts of data across the supply chain, deep learning can help predict demand, optimize stock levels, identify anomalies, and automate complex decisions. Meanwhile, blockchain technology offers a decentralized, immutable, and transparent way to maintain records, making it more reliable and efficient, while simultaneously increasing the transparency and traceability of records and transactions and fostering trust among stakeholders. Blockchain and deep learning have also paved the way for the creation of intelligent supply chain platforms, which not only facilitate secure data sharing but also provide enhanced predictive capabilities, empowering companies to optimize their operations and reduce the risk of disruptions while fostering sustainable manufacturing and logistics. These comprehensive solutions can provide intelligent decision support, transparent transaction management, robust cybersecurity and future-proof cryptographic protection all in one. Building "quantum-resilient," AI-powered blockchain-based systems is just getting more critical as a way to ensure trustworthy, scalable, sustainable and secure supply chain management systems for continued critical industrial operations over the next few decades.

Related work

A. Supply Chain Security

A supply chain security issue arises when the information and physical goods being transported along the supply chain are not protected in terms of confidentiality, integrity, or availability. Mixed-methods studies of technological adoption in the supply chain industry show that the benefits of digitalization depend on trust between supply chain partners, meaning that any compromise in the security of one chain node negatively impacts the other nodes in the chain [1].

A blockchain is a data structure that is replicated and append-only, with blocks of transactions cryptographically chained together by hash pointers and validated according to a distributed consensus protocol (e.g., Proof-of-Work, Proof-of-Stake, Delegated Proof-of-Stake). A proof-of-work or proof-of-stake consensus choice will be prone to quantum attacks, Sybil attacks, centralization pressure, and leader-selection bias, all of which are exacerbated by an adversary gaining access to quantum computing resources [2].

Comparative Analysis

This section presents eight original comparative tables synthesized from the twenty-two reviewed studies. Each table highlights a different analytical dimension, blockchain frameworks, PQC algorithms, deep learning models, application domains, federated learning designs, quantum-secure blockchain strategies, consensus mechanisms, and an integrated advantages/limitations matrix, to support cross-study comparison rather than isolated summaries.

TABLE 1. Comparison of Existing Blockchain Frameworks

Ref.	Framework / Focus	Consensus / Structure	Reported Limitation
[3]	BOVS: blockchain online virtual store for business process management	Standard permissioned ledger	No quantum-resistance consideration

Ref.	Framework / Focus	Consensus / Structure	Reported Limitation
[4]	ML-integrated secure blockchain applications (survey)	Multiple (cross-domain survey)	Heterogeneous evaluation criteria across surveyed systems
[5]	Blockchain-AI synergy for IoT security (review)	Multiple (cross-domain review)	Limited quantitative benchmarking across reviewed schemes
[6]	Blockchain-based IoV security mechanisms (survey)	Consensus latency-sensitive designs	Consensus latency bottleneck for time-critical vehicular tasks
[7]	Multi-level blockchain framework for edge devices	Tiered/hierarchical ledger	Complexity of managing multiple protection tiers
[8]	Quantum-safe Hyperledger Fabric	Permissioned, PBFT-family	Retrofitting overhead for legacy deployments

Proposed Taxonomy

Combining the fourteen literature categories presented in Section 3, this paper provides a new five-tier taxonomy that shows the technological evolution from the base technological competence of deep learning to the ultimate goal of a sustainable supply chain, that is, a secure supply chain.

A. Tier 1 — Deep Learning

The base level includes the model families that are shared across the reviewed studies: recurrent for forecasting [1]; attention-based for forecasting [1]; variational autoencoders for anomaly detection [4]; graph neural networks for relational threat detection [6]. This tier provides the predictive and detective intelligence needed by the higher tiers.

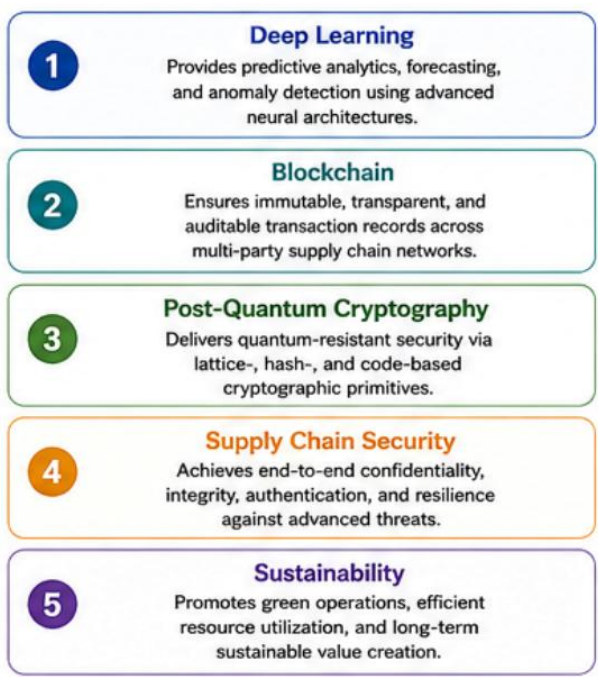

Figure 3. Overall taxonomy showing the five-tier progression from Deep Learning through Blockchain, Post-Quantum Cryptography, and Supply Chain Security, to Sustainability.

B. Tier 2 — Blockchain

The second layer includes distributed ledger architectures that record and validate transactions made or flagged by Tier 1 models, such as permissioned ledgers [5], hierarchical federated ledgers [4] and multi-tier edge ledgers [10]. The tier is designed to turn a model output into something that can be audited and cannot be tampered with.

C. Tier 3 — Post-Quantum Cryptography

The third tier is a quantum adversarial resistant version of Tier 2, which entails lattice based signatures [6] and quantum-safe permissioned-ledger retrofits and quantum-safe identity credentials following the taxonomy of post-quantum versus quantum-native from the survey literature].

D. Tier 4 – Supply Chain Security.

The fourth tier uses the hardened Tiers 1-3 stack for concrete supply chain security problems: transaction verification risk assessment at geospatial scale IoV logistics security and confidentiality for cloud storage.

E. Tier 5 — Sustainability

The top tier is the ultimate goal: a secure supply chain with sustainability features through SDG related forecasting improvements and low energy, quantum resistant consensus design.

Proposed Conceptual Framework

On this taxonomy, this paper suggests a conceptual framework for a Deep Learning based Post-Quantum Blockchain supply chain architecture consisting of nine layers.This paper suggests a nine-layered conceptual framework for a Deep Learning enabled Post-Quantum Blockchain supply chain architecture, based on the provided taxonomy in Section 7. The layers correspond to certain mechanisms presented in the reviewed literature.

1. Data Collection: Raw operational data, shipment record, transaction logs and environmental readings are collected at various points in the supply chain, similar to the sensing inputs in the food-safety monitoring platform [8].
2. IoT Devices: These are physical sensors and RFID/telemetry devices that produce a constant flow of data into the pipeline, just like the multi-level blockchain protection frameworks that address them.
3. Edge Layer: Local computation filters and pre-processes data near its source, which reduces bandwidth and allows the risk-adaptive edge intelligence showcase in federated deep learning frameworks with blockchain integration [2].
4. Deep Learning: Forecasting models, anomaly-detection models and threat-classification models, LSTM variants [1] and variational autoencoders [4] and graph neural networks [6] take raw and pre-processed data and turn it into actionable intelligence.
5. Federated Learning: Model Training can be coordinated across organizational and device boundaries without having to centralize raw data, implement energy-efficient synchronization protocols, and utilize trust-ledger provenance mechanisms like ELCAS and TIMPDL [2].

Conclusions

This review provides an in-depth evaluation of combining deep learning, blockchain, and post-quantum cryptography in modern supply chains. The results show that both technologies have proven themselves as valuable stand-alone technologies. The benefits of deep learning include more accurate demand forecasts, anomaly detection, and intelligent decision-making, while blockchain provides greater transparency, traceability, and data integrity with its decentralized and tamper-proof ledgers. Post-quantum cryptography is a security backbone that is future-proof and can safeguard blockchain systems from quantum computing attacks. Although there are these developments, most of the existing research available explores these technologies on an individual basis and only a handful takes a more holistic approach to their integration into the supply chain context. The review presents a taxonomy and a multi-layer conceptualisation of how deep learning, blockchain, and post-quantum cryptography could contribute to the development of secure, intelligent, and sustainable ecosystems of supply chains.

References

1. N. B. Bhavikatta and N. V. R. Goluguri, "Multi dataset LSTM analysis for accurate and sustainable supply chain forecasting," Discov. Sustain., vol. 7, art. 508, 2026, doi: 10.1007/s43621-026-02828-3.
2. K. Swathi, P. Durga, K. V. Prasad et al., "Secure blockchain integrated deep learning framework for federated risk-adaptive and privacy-preserving IoT edge intelligence sets," Sci. Rep., vol. 15, art. 41133, 2025, doi: 10.1038/s41598-025-24895-8.
3. N. R. Reddy, S. Suryadevara, K. G. R. Reddy et al., "Quantum secured blockchain framework for enhancing post quantum data security," Sci. Rep., vol. 15, art. 31048, 2025, doi: 10.1038/s41598-025-16315-8.
4. G. E. Visuvanathan, M. S. Sayeed, and S. Yogarayan, "BHFVAL: Blockchain-Enabled Hierarchical Federated Variational Autoencoder Framework for Secure Intrusion Detection in Vehicular Networks," Sci. Rep., vol. 15, art. 45742, 2025, doi: 10.1038/s41598-025-28560-y.
5. K. W. Goh, B. U. I. Khan, A. R. Khan et al., "Blockchain-based online virtual store (BOVS): A secure framework for managing machine-created elements in business process management," J. King Saud Univ. Comput. Inf. Sci., vol. 37, art. 276, 2025, doi: 10.1007/s44443-025-00240-x.
6. I. M. Alharbi and N. K. Almazmomi, "AI-optimized blockchain security for smart agriculture using post-quantum cryptography and graph neural network-based threat detection," Peer-to-Peer Netw. Appl., vol. 18, art. 276, 2025, doi: 10.1007/s12083-025-02062-0.
7. H. Saraya, A. Saleh, and A. Rezk, "Geo-Blockchain Intelligence Risk Assessment (GBIRA) technologies for secure and sustainable internet of geospatial big data computing ecosystems: a survey," GeoJournal, vol. 91, art. 43, 2026, doi: 10.1007/s10708-026-11569-9.
8. B. R. Adeyeye and S. A. O. Adeyeye, "Sustainable smart sensing and AI-driven platforms for real-time detection and monitoring of mycotoxins across the food supply chain," Mycotoxin Res., vol. 42, art. 42, 2026, doi: 10.1007/s12550-026-00653-1.
9. C. Meka, K. R. Palakollu, M. Azees et al., "A comprehensive survey on integration of machine learning with secure blockchain-based applications," Cluster Comput., vol. 28, art. 632, 2025, doi: 10.1007/s10586-025-05330-z.
10. D. Kaushik, P. Gulia, N. S. Gill et al., "Synergizing blockchain and AI to fortify IoT security: a comprehensive review," Artif. Intell. Rev., vol. 59, art. 41, 2026, doi: 10.1007/s10462-025-11434-0.