International Journal of Research in Engineering and Management Sciences (IJREMS)
E-ISSN: 3107-7439

Research Article
VOL.: 1, Issue: 5, October 2025

Blockchain–AI Hybrid Models for Supply Chain Security: A Secondary Data Synthesis

[1]Dr. Syed Hassan Imam Gardezi

*[*1]Executive Director and Board Member,Union Investments LLC*

Email: hassanwiz17@hotmail.com

ABSTRACT:

Supply chains all over the world become more computerized, which subjects them to cyber-attacks, fraud, counterfeiting, and data manipulations. Distributed and tamper-evident ledgers are available through blockchain, and predictive analytics, anomaly recognition, and intelligent decision-making is provided by Artificial Intelligence (AI). Hybrid models through the combination of such technologies provide secure, transparent, and adaptive supply chains. The current paper is a synthesis of secondary data (20192025) of scholarly journals, industry reports, and international bodies in order to analyze the value of blockchain-AI hybrid systems in improving the security of the supply chain. We overview the use cases in manufacturing, logistics, pharmaceuticals, and food industries and extract the major areas of integration: blockchain to be more data integrity and provenance, and AI to be more analytics and forecast, risk detection. We introduce a comparative table of blockchain-only, AI-only and hybrid models, conceptual hybrid architecture figure, flow diagram of information flow. The results show that the hybrid systems enhance resilience, detecting fraud, and traceability through the connection between unaltered records and adaptive intelligence. Scalability, interoperability, governance and data quality continue to be problematic. The way forward in work should be the standardization of interfaces, guarantee privacy, and create cross-sector models of reliable hybrid supply chain.

Keywords: Regulatory Compliance, Cryptographic Techniques, Immutable Records, Data Encryption, Tokenization, Blockchain Auditing, Privacy-Preserving Blockchain, Distributed Ledger Technology (DLT), Financial Privacy.

Received Date: 5 October 2025**; Accepted Date:** 15 October 2025**; Published Date:** 20 October 2025.

Introduction

The contemporary supply chains are complicated, international, and data-oriented. Digitization enhances efficiency, but it also offers more weaknesses: there are cyberattacks, fake products, insider threats, and no end-to-end visibility (World Economic Forum, 2023). The blockchain technology offers tamper-evident distributed registries to secure the supply chain dealings, with the artificial intelligence techniques developing in real-time decisions, anomaly detection, and predictions (Wamba and Queiroz, 2020; Kshetri, 2021). AI and blockchain contain weaknesses in their individual applications. Blockchain is trustful and immutable but they lack smart analytics, whereas AI models require quality and integrity of data (Bodkhe et al., 2020). The combination of the two technologies enables blockchain to ensure the availability of credible data input, whereas AI derives useful intelligence on the data (Biswas et al., 2023). This is a hybrid approach that enhances the

security of supply chains by integrating immutable data recording and predictive and adaptive intelligence.

2. Background of the Study

Product provenance, anti-counterfeiting, and traceability are the most common uses of blockchain in supply chains, particularly with food, pharmaceutical, and luxury products (Tönnissen & Teuteberg, 2020). Hyperledger, Ethereum, and blockchains on private network have been implemented to store logistics and certification information. The applications of AI have been in the demand forecasting, anomaly detection, fraud detection, and optimization. As an example, cold chains monitor abnormal shipping behaviors or sensor malfunctions, which is identified by machine learning algorithms (Ivanov et al., 2022). The latest trends suggest hybrid systems of blockchains and AI, in which blockchain guarantees the impossibility of non-cryptographically altered data streams and AI facilitates smart analytics (Salah et al., 2021). Such systems are useful in real-time risk identification, provenance, and response.

3. Justification

Crossbreeding of blockchain and AI is a relatively recent phenomenon, and the amount of secondary data is rich in this case, namely academic articles, case studies in the industry (IBM Food Trust, TradeLens), policy reports (OECD, WEF). Primary data collection on multinational supply chains is costly and usually sensitive and therefore synthesizing on secondary offers a sound and holistic perspective of the way these technologies are being integrated in practice and research.

4. Objectives of the Study

The study aims to:

1. Review blockchain and AI applications in supply chain security using secondary data.
2. Identify integration models and architectures for hybrid blockchain–AI systems.
3. Compare blockchain-only, AI-only, and hybrid models in terms of capabilities and limitations.
4. Present conceptual architecture and information flow diagrams for hybrid systems.
5. Identify challenges and future research directions.

5. Literature Review

Security in Supply Chains performed using blockchain:

The use of blockchain technology in supply chains is essential in the guarantee of data immutability, transparency, and decentralized trust. Through the distributed ledger mechanisms, blockchain will ensure that records cannot be tampered with unauthorized, and it offers a verifiable history of each transaction and product movement (Kshetri, 2021; Salah et al., 2021). The requirement is especially relevant to the industries where the traceability as well as the provenance is essential, including food, pharmaceuticals, and logistics. Blockchain enhances accountability since all transactions and events are documented in a common ledger and facilitate real-time verification of the supply chain operations.

Artificial Intelligence (AI) to support Intelligent Analytics and Risk Detection:

Artificial Intelligence (AI), on the contrary, is adding analytical intelligence to the supply chain by identifying anomalies, predicting risks, and advising strategic or operational decisions (Queiroz and Wamba, 2022). The logistics data can be recognized as abnormally patterned, delays or failures can be predicted, and the decision-making processes can be optimized in real time using the machine learning models. In contrast to blockchain, where data integrity and transparency are considered to be the main concerns, AI provides an additional intelligence layer, i.e., allowing predictive maintenance, fraud detection, and adaptive security responses.

Development of Hybrid Blockchain-AI Systems:

In the present situation, the emergence of hybrid systems that bring the advantages of blockchain and AI has taken place to create more secure and efficient supply chains. As an illustration, IBM Food Trust combines blockchain-based end-to-end traceability with AI-based software to evaluate the risk of contamination in food supply chains. Equally, the TradeLens platform, a service of Maersk and IBM, uses blockchain to provide safe shipping records but uses AI analytics to find anomalies in logistics processes. Blockchain in pharmaceutical cold chains can provide the safety of sensor data, and AI will identify temperature anomalies that may compromise the safety of the products (Biswas et al.,

2023). These practical applications show the increased practical usefulness of hybrid solutions.

Patterns of integration that have been identified in Literature:

According to the secondary literature, three major patterns in terms of integrating blockchain-AI hybrid systems can be identified. The former is the Blockchain feeding AI in which trusted blockchain information is used as an input to machine learning models, enhancing model reliability and provenance. The second one is AI feeding Blockchain where AI outputs, e.g. anomaly alerts or predictive insights, can be used to execute smart contracts or automatically document decisions to the blockchain. The third trend is the co-processing, in which AI models are directly integrated into the blockchain-enabled Internet of Things, which enables real-time data processing and modification at the same time. These trends indicate varying degrees of technological incorporation, with each of them having its own security and performance benefits.

Material and Methodology

The proposed study is grounded in the secondary data and is primarily aimed at synthesizing the available research and reports, instead of gathering primary data. This was to explore the use of blockchain-AI hybrid models in supply chain security using valid, varied, and well-documented sources. The content analysis procedure was systematic in order to collect, screen and interpret information.

Input:
S = {s1, s2, ..., sn} // Real-time IoT sensor data
B = Blockchain ledger
M = Trained AI/ML anomaly detection model

Output:
Secure, traceable alerts and immutable transaction records

1. Collect real-time sensor data di from each node si ∈ S.
2. Validate di for completeness and format.
3. For each di:
Create transaction Ti = Hash(di)
Submit Ti to blockchain B
If confirmed, append Ti to distributed ledger
Else, flag error and discard di
4. Retrieve newly added block data Dblock from B.
5. Preprocess Dblock (cleaning, feature extraction).
6. Apply AI model M on Dblock.
7. If anomaly or risk detected:
Generate alert Ai with timestamp
Record Ai on blockchain for immutability
Trigger smart contracts or notify stakeholders
8. Else, continue monitoring.

The algorithm outlines the general method of computation of blockchain-AI hybrid systems of supply chain security. It begins with the data retrieval, then permanent storage, access and pre-processing, unexpected event detection using AI, and lastly notification and automatic reaction. Such an illustration fits common methodology in computer science research since it contains a very

straightforward step-by-step pseudo-code algorithm, which can be executed in any programming or simulation context.

Academic Sources:
The articles of peer-reviewed journals and conferences papers were gathered in big databases like IEEE Xplore, Elsevier (ScienceDirect), and Springer during the time frame 2019-2025. These sources offered both theoretical background and technical paradigms and empirical evidence on blockchain, AI, and how these technologies work together in supply chains. Relevant publications were found by the use of keywords and Boolean search strategies.

Industry Whitepapers:
Sources such as reports and technical white papers of major organizations such as IBM, Maersk, and Oracle were reviewed to know how it was done in real life, pilot project, and enterprise level solutions. Such documents usually referred to architectural blueprints, case studies and performance measure that supplemented scholarly conclusions.
International: International Accounting Standards Board, 2010, p.1.; Policy: HM Revenue and Customs, 2010, p.1.; and International Accounting Standards Board, 2010, p.1.
International agency reports as reports of OECD and World Economic Forum (WEF) were also used in secondary data. Through these policy documents, the company was able to gain insight into the global trends, regulatory challenges, and strategic view of the supply chain security and the emerging technologies.

Standards and Regulatory Documents:
The ISO/TC 307 standards and guidelines relevant to the subject were reviewed to gain knowledge of formal definitions, interoperability, and best practices of blockchain and AI systems in supply chains.

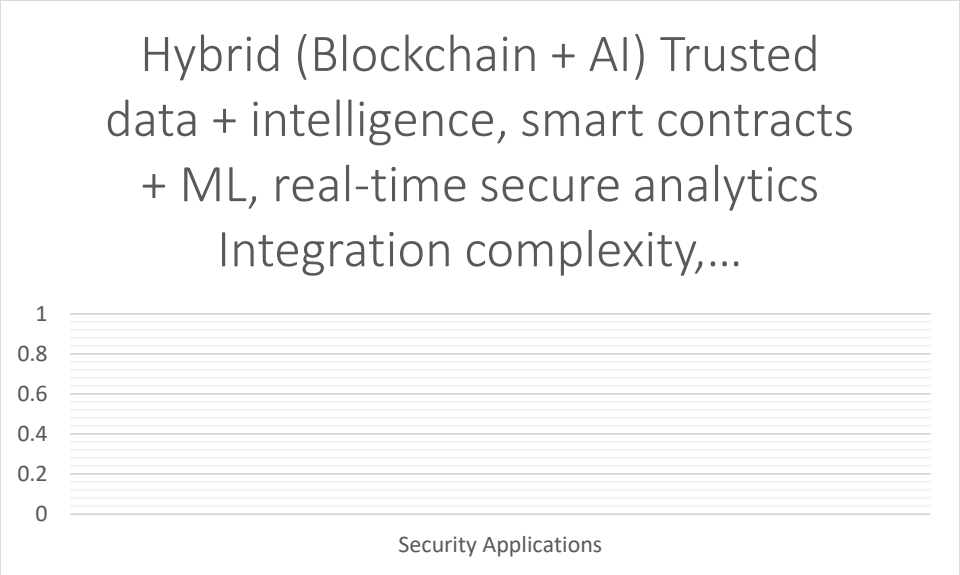
Data Analysis Approach:
The information was organized into major categories and the analysis of documents was presented in the form of a structured document, which included such aspects: technology use (blockchain, AI, hybrid), sectoral application (e.g., logistics, manufacturing, pharmaceuticals), and security functions (traceability, anomaly detection, provenance, fraud prevention). Coding and comparative analysis of thematic patterns, gaps and integration models were identified.
Synthesis: Even though this is not a visual art, it conveys the concept through visual means, since the imagery of the artwork is striking and the metaphorical meaning clear. Visualization and Synthesis: Although it is not visual art, it expresses the idea visually, as the imagery of the piece of art is impressive and the metaphorical one is evident.
On the basis of the processed data, tables, figures, and flowcharts were created to generalize the results, describe the conceptual architectures, and represent the flow of information between blockchain and AI elements. This systematic approach to the synthesis of the available secondary evidence was what made it deep and clear.

7. Results and Discussion

7.1 Comparative Table

Table 1: Blockchain vs AI vs Hybrid Models in Supply Chain Security

Model Type	Strengths	Limitations	Security Applications
Blockchain-only	Data integrity, provenance, transparency	No analytics, scalability issues, static rules	Anti-counterfeiting, traceability
AI-only	Predictive analytics, anomaly detection	Data manipulation risk, lack of trust layer	Fraud detection, demand forecasting
Hybrid (Blockchain + AI)	Trusted data + intelligence, smart contracts + ML, real-time secure analytics	Integration complexity, governance, interoperability	End-to-end secure, intelligent, traceable supply chains



The combination of AI and blockchain in the security of the supply chain is a great synergy of trust and intelligence. As shown on the chart, blockchain-based hybrid models are a combination of unaltered data integrity and predictive analytics of AI, allowing real-time analytics, anomaly detection, and automated decision-making. Although such issues as complexity of integration and governance still exist, this solution guarantees end-to-end traceability, fraud prevention, and smarter logistics on a global network.

7.2 Conceptual Hybrid Architecture

Figure 1: Blockchain–AI Hybrid Architecture for Supply Chain Security

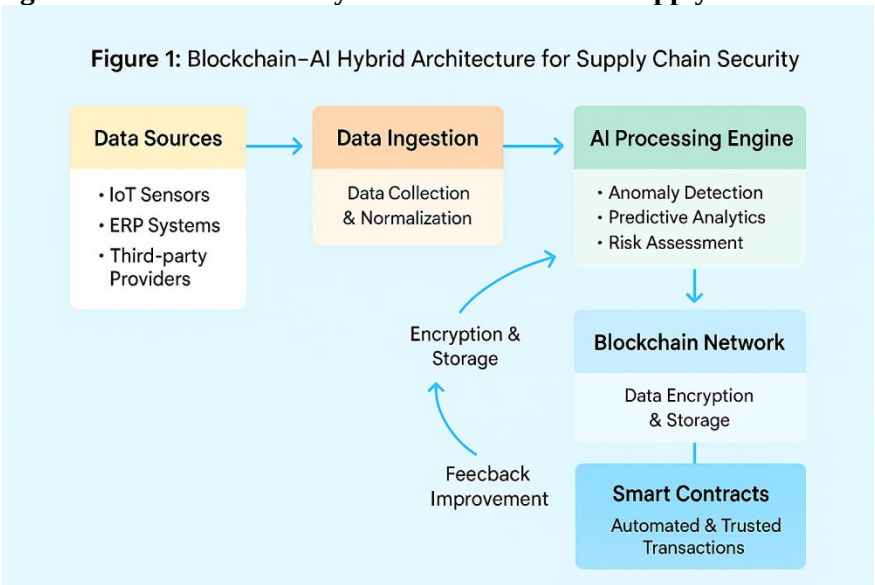
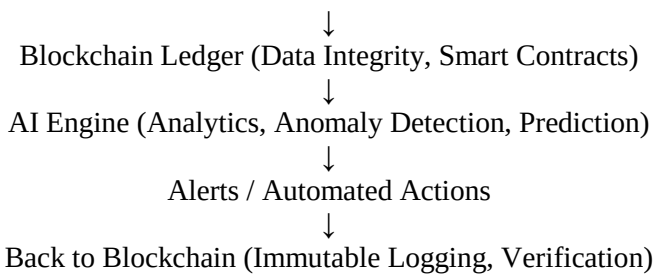


Figure 1: Blockchain–AI Hybrid Architecture for Supply Chain Security, Sneha — designed to highlight the layered integration of IoT, AI, and blockchain across the supply chain.

7.3 Flowchart of Blockchain–AI Information Flow

Figure 2: Blockchain–AI Integration Flow for Secure Supply Chains



This flow shows how sensor-based data is safely analyzed and processed to do something based on a hybrid of both blockchain and AI technology:
Sensor/IoT Data: IoT devices record real-time data of assets in the supply chain (e.g., temperature, location, vibration).
Blockchain Ledger:To provide integrity and traceability and provide smart contracts that allow automated compliance and transactions, data is recorded permanently.
AI Engine:The data obtained is processed with the help of AI to detect anomalies, forecast and predict risks.
Alerts / Automated Actions: Depending on the insights of AI, the system issues warnings or performs smart contract-based functions (e.g., rerouting, notifying suppliers).
Back to Blockchain: Every action and decision is registered indelibly so that they can be audited, verified and learnt continuously.

7.4 Key Findings

- Hybrid models improve trust, traceability, and threat detection by combining blockchain's immutability with AI's intelligence.
- Secondary evidence shows reduced fraud incidents, improved real-time visibility, and enhanced regulatory compliance (OECD, 2024; WEF, 2023).
- Major challenges include interoperability between blockchain platforms, explainability of AI decisions, data privacy, and governance of shared infrastructure (Queiroz & Wamba, 2022).

8. Limitations of the Study

This study relies entirely on secondary sources. Many hybrid model deployments are pilots or proprietary, limiting publicly available performance data. Sector-specific results may not generalize globally. No primary data collection or experiments were conducted.

9. Future Scope

Future research should:

- Develop standardized interfaces and data schemas for hybrid models;
- Integrate privacy-preserving AI (e.g., federated learning) with blockchain;
- Explore interoperability between public and private chains;
- Establish governance frameworks for cross-organization hybrid systems;
- Conduct longitudinal impact studies.

10. Conclusion

Blockchain–AI hybrid models represent a promising paradigm for securing global supply chains. Blockchain provides tamper-proof, transparent data records, while AI enhances decision-making and threat detection. Together, they enable secure, intelligent, and adaptive supply chains capable of responding to evolving risks. While technical, governance, and interoperability challenges remain, secondary evidence suggests that hybrid systems outperform blockchain-only or AI-only models in traceability, fraud prevention, and resilience.

References

1. Biswas, B., Muthukkumarasamy, V., & Suryani, E. (2023). Blockchain–AI synergy for secure supply chains. IEEE Access.
2. Bodkhe, U., et al. (2020). Blockchain for IoT-based supply chains. IEEE Communications Surveys & Tutorials.

3. IBM. (2022). IBM Food Trust: Blockchain for Food Safety and Traceability.
4. Ivanov, D., Dolgui, A., & Sokolov, B. (2022). Supply chain resilience and AI. Int. Journal of Production Research.
5. Kshetri, N. (2021). Blockchain's roles in strengthening supply chains. Journal of Business Research.
6. OECD. (2024). Emerging technologies and supply chain security.
7. Queiroz, M. M., & Wamba, S. F. (2022). Blockchain and AI in supply chain management. International Journal of Logistics Management.
8. Salah, K., et al. (2021). Blockchain–AI integration frameworks. Future Generation Computer Systems.
9. Tönnissen, S., & Teuteberg, F. (2020). Analysing the impact of blockchain on supply chains. Computers & Industrial Engineering.
10. TradeLens. (2023). Blockchain and AI in maritime logistics. Maersk.
11. Wamba, S. F., & Queiroz, M. M. (2020). Smart supply chains with blockchain and AI. Business Horizons.
12. World Economic Forum. (2023). Building cyber-resilient supply chains.
13. ISO/TC 307. (2024). Blockchain and distributed ledger technologies — Standards Roadmap.