



REVIEW

Applications of AI and Blockchain in Origin Traceability and Forensics: A Review of ICs, Pharmaceuticals, EVs, UAVs, and Robotics

Hsiao-Chun Han¹, Der-Chen Huang^{1,*} and Chin-Ling Chen^{2,*}

¹Department of Computer Science and Engineering, National Chung Hsing University, Taichung City, 40227, Taiwan

²Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung City, 41349, Taiwan

*Corresponding Authors: Der-Chen Huang. Email: huangdc@cs.nchu.edu.tw; Chin-Ling Chen. Email: clc@mail.cyut.edu.tw

Received: 28 July 2025; Accepted: 25 September 2025; Published: 30 October 2025

ABSTRACT: This study presents a systematic review of applications of artificial intelligence (abbreviated as AI) and blockchain in supply chain provenance traceability and legal forensics cover five sectors: integrated circuits (abbreviated as ICs), pharmaceuticals, electric vehicles (abbreviated as EVs), drones (abbreviated as UAVs), and robotics—in response to rising trade tensions and geopolitical conflicts, which have heightened concerns over product origin fraud and information security. While previous literature often focuses on single-industry contexts or isolated technologies, this review comprehensively surveys these sectors and categorizes 116 peer-reviewed studies by application domain, technical architecture, and functional objective. Special attention is given to traceability control mechanisms, data integrity, and the use of forensic technologies to detect origin fraud. The study further evaluates real-world implementations, including blockchain-enabled drug tracking systems, EV battery raw material traceability, and UAV authentication frameworks, demonstrating the practical value of these technologies. By identifying technological challenges and policy implications, this research provides a comprehensive foundation for future academic inquiry, industrial adoption, and regulatory development aimed at enhancing transparency, resilience, and trust in global supply chains.

KEYWORDS: AI; blockchain; preparation; ICs; pharmaceuticals; EVs; drones; robotics

1 Introduction

In the late 20th century, a surge in free trade and economic globalization prompted U.S. corporations to pursue “maximum profit and minimum cost” by outsourcing key functions—including procurement, manufacturing, and R&D—to multinational suppliers with greater price competitiveness. This shift gave rise to global value chains and a complex system of international labor divisions that span multiple countries and production stages. However, it also incurred significant economic repercussions, such as a mounting U.S. trade deficit, domestic industrial hollowing, and widespread job displacement, leading to trade frictions. Furthermore, the broader geographical span and growing complexity of goods flows have intensified concerns about opacity in supply chain processes. In recent years, the Russia-Ukraine war has leveraged unmanned aerial vehicles and the Starlink satellite system to reshape military operations, significantly increasing demand for related technologies and underscoring the imperative of securing critical supply chains during geopolitical conflicts. Key industries—including pharmaceuticals, electric vehicles, drones, robotics, and ICs—have become central to technological development and are projected to gain strategic influence ([1–5], see Fig. 1 below). Nevertheless, their production remains highly dependent on imported



raw materials ([6], see Fig. 2 below), posing national security risks. In response, the U.S. government has sought to reshore these industries and, amid rising concerns over information security, has intensified efforts to combat illicit practices such as origin fraud. These efforts involve enhancing component traceability and strengthening legal and forensic safeguards.

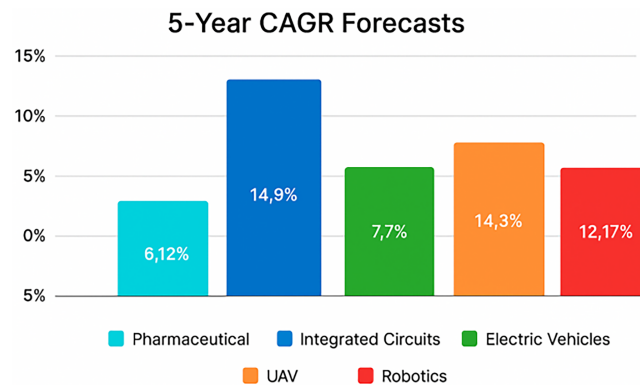


Figure 1: Annual growth rates projected for the five industries over the next five years

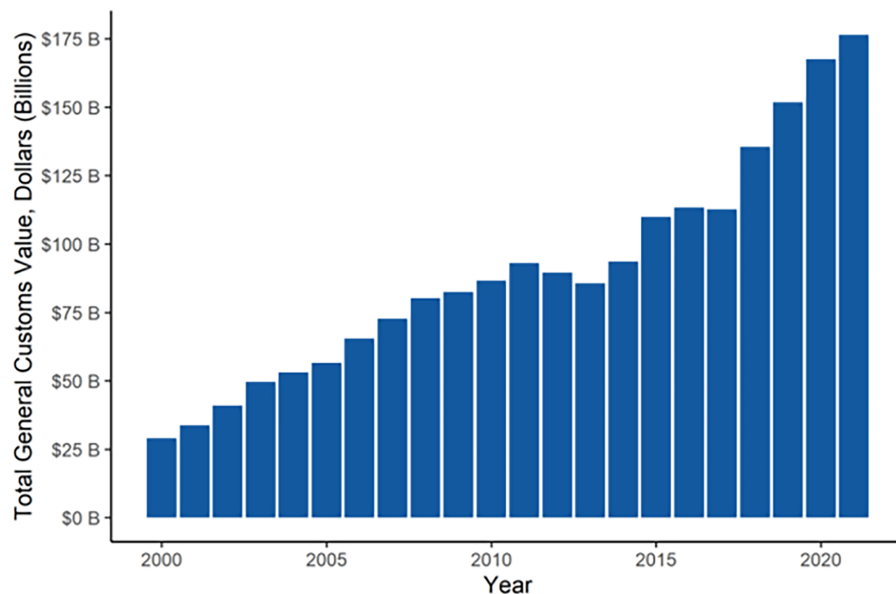


Figure 2: Continued increase in U.S. pharmaceutical import value

- (a) ICs are essential components of all electronic products and constitute one of the most critical points of cybersecurity vulnerability. If malicious code is embedded and activated at a crucial moment, it can take over system control, thereby posing severe security risks to a wide range of electronic systems. For example, the Spanish cybersecurity firm Tarlogic Security has identified hidden instructions in Chinese-manufactured ESP32 chips, which could function as backdoors, potentially allowing the covert remote control of millions of IoT devices [7], including EVs, UAVs, and robotics systems.
- (b) The prevalence of counterfeit pharmaceuticals poses a critical threat to global public health, resulting in an estimated 110,000 deaths in the United States in 2023 alone [8] and approximately one million deaths worldwide each year [9]. In developing countries, one in ten medical products is counterfeit

or substandard [10], with up to 30% of pharmaceuticals in regions such as Africa, Asia, and Latin America failing to meet regulatory standards [11]. Likewise, major disasters and widespread infectious disease outbreaks frequently lead to drug shortages, heightening social anxiety and unrest [12]. This vulnerability is further exacerbated under intensified geopolitical tensions, prompting governments around the world to enact pharmaceutical traceability regulations aimed at enhancing transparency across supply chains [13–16].

- (c) Instability in component supply can lead to significant disruptions in automotive production activities [17], with amplified implications for national security during periods of geopolitical conflict. Furthermore, EVs, which possess integrated capabilities for data collection and surveillance, may be vulnerable to exploitation or remote manipulation by adversarial entities. Consequently, the stability and transparency of the sourcing of EV components have emerged as critical strategic concerns. Among all components, the battery is arguably the most vital; however, its supply chains of raw materials have been repeatedly linked to violations of human rights and environmental degradation [18]. In response, leading nations have implemented legislative frameworks mandating traceability and strict regulatory oversight of EV components and raw materials, aiming to prevent fraudulent practices such as country-of-origin misrepresentation [19–21].
- (d) Currently, large UAVs are primarily deployed for military and governmental purposes. In particular, during the Russia-Ukraine war, UAVs have demonstrated significant effectiveness in striking tanks and air defense systems, as well as in executing reconnaissance and electronic warfare missions. As such, UAV-based tactics are increasingly regarded as a critical component of future warfare strategies. However, if these systems are compromised or remotely controlled by adversarial actors, they could become offensive weapons against their own forces. In response to these risks, countries such as the United States, the European Union, and Japan have increased the regulatory oversight of the supply of UAV components and the integrity of the system [22–25].
- (e) Robots are widely deployed across a wide range of sectors, including manufacturing lines, seaports, automated warehouses, customer service, and even personal companionship. Designed for continuous and long-term operation, these systems are inherently vulnerable to cyber intrusions, rendering them potential targets for adversarial infiltration. If backdoors are implanted or remote attacks initiated by hostile actors, robots can be able to immediately disrupt port logistics, cripple factory operations, damage medical infrastructure, or even target specific individuals. Such scenarios pose serious threats to public safety and economic stability and may ultimately influence the outcomes of geopolitical conflicts. In response, leading countries such as the United States, the European Union, and Japan have introduced legislation aimed at reinforcing supply chain autonomy and enhancing cybersecurity in the robotics sector [22–25].

The supply chains of these industries are inherently complex and globally distributed, presenting significant challenges in the identification and traceability of the origin of material. Addressing these issues increasingly relies on the adoption of emerging technologies, particularly blockchain and AI. In recent years, the integration of AI and blockchain in supply chain management has expanded considerably. AI contributes to a wide range of operational improvements, including forecasting market demand, inventory and warehouse optimization, transportation and logistics efficiency, risk analysis of disruptions, anomaly detection, and intelligent procurement. In parallel, blockchain technology—characterized by its decentralized architecture and immutability—ensures the authenticity and integrity of provenance data, while facilitating the automated execution of smart contracts and inter-node protocols across distributed systems. Therefore, the integration of AI and blockchain technologies into key sectors—such as ICs, pharmaceuticals, EVs, UAVs, and robotics—can substantially strengthen the control and verification of product provenance. Similarly,

country-of-origin fraud is considered a criminal offense under both criminal and tax legislation, and has been subject to increasingly stringent legal penalties and enforcement measures in many jurisdictions. As a result, the role of forensic technologies in supporting legal investigations and evidence collection has gained increasing importance. Among these sectors, ICs—given their central role in the electronics industry and their critical implications for information security—have become a primary focus of traceability enforcement and serve as vital media for recording provenance evidence through forensic methodologies. In light of these developments, the objectives of this study are as follows (see [Table 1](#) below):

Table 1: Research questions and objectives for the survey

	Research Question	Objective
1	What are the current approaches to integrating AI and blockchain technologies for supply chain traceability in pharmaceuticals, electronic vehicles, UAVs, robotics, and ICs?	Consolidate the technological architectures proposed across various academic studies—such as smart contracts, federated learning, private blockchain, and digital twins—and examine how these technologies are implemented and integrated within the aforementioned industries.
2	What are the specific application domains of these technologies within each industry, and what empirical case studies have been reported?	To review representative application cases—such as pharmaceutical anti-counterfeiting registration, battery source tracking, UAV component verification, robotic manufacturing forensics, and IC authenticity validation—and to outline how AI and blockchain technologies are employed to realize these functions.
3	Can the integration of AI and blockchain technologies enhance supply chain transparency, improve anti-counterfeiting capabilities, and strengthen the effectiveness of forensic evidence documentation? What tangible outcomes have been demonstrated?	Examine the practical effectiveness of relevant technologies, as documented in the literature, in addressing issues such as counterfeit pharmaceuticals, country-of-origin fraud, material traceability, and preservation of forensic evidence for legal proceedings.
4	What potential challenges and methodological limitations remain unaddressed in the aforementioned applications?	Synthesize the challenges identified in existing research, including data reliability, consensus mechanism efficiency, barriers to cross-border collaboration, regulatory compliance difficulties, system interoperability, and security vulnerabilities.

(Continued)

Table 1 (continued)

	Research Question	Objective
5	What are the research gaps and development opportunities for the integrated application of AI and blockchain technologies in cross-sector and multi-industry contexts?	In-depth analysis reveals key opportunities for advancement, including the lack of unified cross-industry platforms, limited multi-stakeholder experimentation and comparative studies, and the need to integrate forensic data, establish standardized smart contracts, conduct real-world pilot testing, and adapt regulatory frameworks.
6	Based on the research findings, what practical recommendations can be offered to inform academic inquiry and policy development?	Insights derived from the literature suggest the need to support AI-blockchain-based policy frameworks—such as battery passports, pharmaceutical traceability regulations, and IC export verification mechanisms—as well as to develop collaborative models among academia, industry, and government, and to promote standardized frameworks for international supply chain transparency.

- (a) Conduct a systematic review of the literature on the current applications of AI and blockchain technologies in supply chain management and product provenance traceability, with a particular focus on high-risk and high-sensitivity industries such as ICs, pharmaceuticals, electric vehicles, UAVs, and robotics.
- (b) Examine traceability control mechanisms for ICs and explore how forensic technologies can be used to record provenance evidence and detect country-of-origin fraud.

This study synthesizes existing academic research by describing technological architectures, key application domains, and the prevailing research trends. In addition, it evaluates the practical effectiveness and challenges of these technologies in enhancing supply chain transparency, preventing origin-related fraud, improving security resilience, and preserving legal forensic evidence. The goal is to provide an integrated knowledge base and practice-oriented recommendations to support future research and policy development.

1.1 Research Scope

In recent years, the integrated application of AI and blockchain has attracted growing academic interest, with supply chain management emerging as a particularly critical domain. This technological convergence addresses multiple core challenges, including data transparency, product traceability, transactional trust, security, and regulatory compliance. The existing literatures have thoroughly examined the architectural models and potential benefits of AI-blockchain integration (see [Table 2](#) below). For example, studies such as [26,27] provide systematic reviews of how these technologies enhance security, intelligent decision-making, and operational transparency. Nevertheless, much of the current research remains confined to single-industry contexts or narrowly focused technical perspectives. Some studies emphasize how AI can improve blockchain efficiency—through improvements in consensus mechanisms or data privacy protection [28]—while others are limited to applications in specific sectors, such as healthcare and finance [29,30].

Despite increasing scholarly interest in AI and blockchain technologies, there still have a notable lack of comprehensive review studies that address their integrated application within the supply chains of five geopolitically sensitive and security-critical industries: ICs, pharmaceuticals, electronic vehicles, UAVs, and robotics. Specifically, current literatures have not offered a consolidated overview of how these technologies can be used to enhance data reliability, provenance traceability, anomaly detection, and access control in these high-risk sectors. In addition, the role of forensic technologies in detecting and preventing country-of-origin fraud has received insufficient academic attention.

Taking UAVs as an example, prior research, such as Ref. [31], has conducted in-depth analyses on the application of blockchain in drone communications and cybersecurity. In the context of EVs, Ref. [32] explores the integration of AI and blockchain for charging optimization and energy distribution. The study [33] investigates the use of blockchain to improve security and transparency within the robotics supply chain. In the pharmaceutical sector, Ref. [34] examines the challenges and potential of applying these technologies to combat counterfeit drugs and ensure traceability. Building on these efforts, this study aims to comprehensively review and synthesize academic research on the integration of AI and blockchain in the supply chains of five geopolitically sensitive and security-critical industries: ICs, pharmaceuticals, EVs, UAVs, and robotics. Particular attention paid to the technological integration methods, representative application scenarios, and the challenges encountered in real-world implementations. In doing so, this study addresses current gaps in the literature concerning cross-sectoral applications, systematic knowledge consolidation, supply chain traceability, cybersecurity, and forensic verification. The purpose of this project is to provide a conceptual foundation for future academic research and to inform practical policy development.

Table 2: Comparison between AI/Blockchain/supply chain surveys

Title/Year	Objective	Merits	Demerits	1	2	3	4	5	6
AI-Enhanced Blockchain Technology: A Review of Advancements and Future Directions (2022) [26]	To provide a comprehensive overview of how AI enhances blockchain	The integration of ML/DL/NLP/DR with blockchain	Not tailored to specific industry contexts	N	Y	N	Y	Y	N
A Critical Analysis of the Integration of Blockchain and AI in Supply Chains (2021) [27]	A review of the applications and emerging trends of AI and blockchain in SCM	Identify integration challenges and future directions for SCM	Lack of detailed technical classification and comparative analysis of applications	N	Y	N	N	N	N
Technological Convergence of Blockchain and Artificial Intelligence: A Comprehensive Survey (2023) [28]	The integrated development and challenges of blockchain and AI	Encompassing technologies, applications, challenges, and future developments	Lack of implementation validation and application classification tables	N	Y	N	Y	Y	Y

(Continued)

Table 2 (continued)

Title/Year	Objective	Merits	Demerits	1	2	3	4	5	6
A Review of Blockchain Technology, Current Challenges, and AI Integration (2021) [30]	Examine methods by which AI enhances the blockchain	To elaborate on how AI addresses the challenges faced by blockchain	Technologically focused, with no reference to industry-specific applications	N	Y	N	Y	Y	N
Blockchain Meets Machine Learning: A Survey (2023) [29]	Explore applications of ML and blockchain across multiple domains	Covering the advantages and challenges in SCM, finance, and security	Lack of comprehensive technical and methodological classification	N	Y	N	N	N	N
On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective about Security (2022) [35]	Security issues arising from the integration of AI and blockchain	Including risks, ethics, regulatory frameworks, and governance	Lack of categorization and application mapping	N	Y	N	N	N	N
A Comprehensive Review on Artificial Intelligence and Blockchain Technologies for EV Charging (2023) [36]	Explore the application of AI and blockchain in EV charging systems	Focusing on energy scheduling, demand forecasting, and cybersecurity in EV	Focused on a single application, lacking categorical analysis	N	Y	N	N	N	N
Optimizing Demand Response and Load Balancing in Smart EV Charging Networks Using AI Integrated Blockchain Framework (2024) [32]	Proposes an AI-blockchain-based framework for load balancing in EV	Provides evidence for improving efficiency and security	Focused on specific architectures, lacking a broad-based review	N	Y	N	N	N	N

(Continued)

Table 2 (continued)

Title/Year	Objective	Merits	Demerits	1	2	3	4	5	6
Blockchain and AI in Pharmaceutical Supply Chain (2024) [34]	Proposes an AI-blockchain-based system for pharmaceutical safety tracking	Including prototype implementation and DApp	A non-systematic literature review lacking categorical organization	N	Y	N	N	N	N
Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey (2022) [31]	Explores the application of blockchain in UAV network communications and cybersecurity	Covers UAV characteristics, challenges, architectural, and blockchain integration	Lacks an AI perspective, with a primary focus on security protocols	N	Y	Y	Y	Y	Y
A Survey of Blockchain and Artificial Intelligence for 6G Wireless Communications (2023) [37]	Analyzes the application of AI and blockchain in UAV communications over 6G networks	The integration of technologies for spectrum management, privacy, and security	The content is primarily forward-looking and has yet to be empirically validated	Y	Y	Y	Y	Y	Y
A Survey on Blockchain in Robotics (2021) [33]	Explores the applications and challenges of blockchain in robotics	cybersecurity issues in robotics and the corresponding blockchain-based solutions	Lacks AI integration and systematic comparison	N	Y	N	N	N	N

Note: 1: 5G-focused, 2: AI/Blockchain-focused, 3: UAV-focused, 4: Taxonomy available, 5: Comparative analysis with other approaches using tables, 6: Categorization of approaches.

1.2 Contributions

Although numerous studies have conducted comprehensive reviews on the integration of AI and blockchain—highlighting their potential in supply chain security, privacy protection, and intelligent decision-making—most of the existing literature remains focused on individual technological aspects, individual industries, or specific data processing techniques. To date, there has been no holistic synthesis that addresses the application of AI and blockchain in supply chain traceability and legal forensics in high-sensitivity sectors such as ICs, pharmaceuticals, EVs, UAVs, and robotics. Consequently, the main contributions of this study are as follows.

- (a) Consolidate the roles of AI and blockchain within the supply chains of ICs, pharmaceuticals, EVs, UAVs, and robotics. This study aims to establish a comprehensive, cross-sectoral research framework that addresses the fragmented and siloed nature of the existing literature.

- (b) Identify the predominant integration models and critical applications of AI and blockchain in these industries. Prior studies are systematically categorized according to their application domains, core technological architectures (e.g., smart contracts, federated learning, private blockchains), and functional objectives (e.g., provenance traceability, criminal forensics, information transparency, anomaly detection, and privacy protection).
- (c) Propose future research directions and key challenges for the integrated application of AI and blockchain in high-risk supply chains. This study also critically examines the methodological, practical, and structural limitations identified in representative works—for example, the lack of longitudinal traceability in high-risk supply networks or the absence of industry-specific integration strategies, as observed in [31,33,34].

For policy implications, beyond its academic contributions, this study also carries several important policy implications for industries, regulators, and governments. First, the five sectors examined in this review—ICs, pharmaceuticals, EVs, UAVs, and robotics—share common vulnerabilities in origin opacity, which can result in national security risks, counterfeit circulation, and reduced trust in global value chains. Policymakers should therefore prioritize the establishment of standardized provenance frameworks that enable transparent, interoperable, and verifiable records of component origins. Second, regulatory authorities such as the FDA, EU Commission, and civil aviation agencies must consider adopting blockchain-based provenance models (e.g., drug traceability under DSCSA or EV “battery passports”) as enforceable compliance tools, ensuring that traceability requirements are consistently met across jurisdictions. Third, governments should encourage cross-industry collaboration in setting data standards, since heterogeneous supply chains often face fragmented reporting practices and inconsistent provenance requirements. Finally, by embedding AI-driven anomaly detection and blockchain-enabled forensic verification into legal frameworks, states can strengthen their ability to deter illicit practices such as origin fraud, adversarial component insertion, and counterfeit drug distribution. These policy insights underscore that AI–blockchain integration is not only a technical solution but also a regulatory enabler, with direct relevance to national security, public health, and industrial resilience.

1.3 Organization and Reading Map

The structure of this study and the organization of the remaining sections are as follows (see Fig. 3 below):

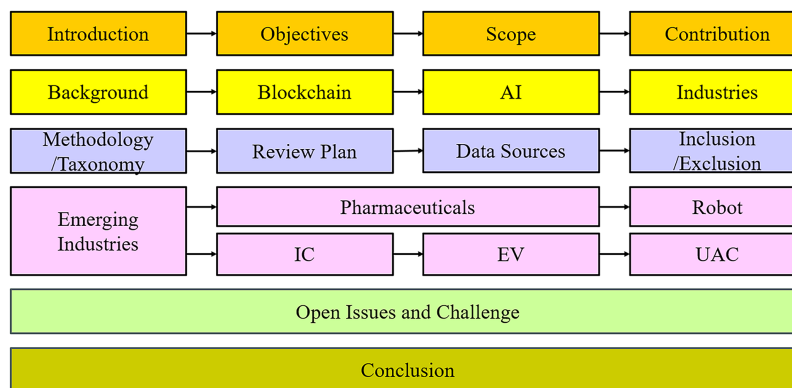


Figure 3: Structure and organization of this study

[Section 2](#) reviews the background of AI and blockchain applications in supply chain management, and of 5 security-critical industries: ICs, pharmaceuticals, EVs, UAVs, and robotics to provide a technical overview and outline the key challenges facing each sector.

[Section 3](#) describes the research methodology used in this study, which is grounded in a Systematic Literature Review (abbreviated as SLR). This section details the database search procedures, Boolean query formulations, inclusion and exclusion criteria, and the classification dimensions and processing workflow used for analysis.

[Section 4](#) synthesizes the current academic literature on AI and blockchain integration in the supply chains of the aforementioned industries, highlighting development trends and representative applications in various domains.

[Section 5](#) discusses unresolved research issues and practical barriers identified in the existing literature, and proposes potential future research directions and development strategies.

[Section 6](#) concludes the study by summarizing its key contributions and emphasizing the academic and practical implications of integrating AI and blockchain in the supply chains of high-sensitivity industries.

The primary abbreviations used in this study and their corresponding meanings are summarized in [Table 3](#) (see [Table 3](#) below).

Table 3: Descriptions of all English abbreviations

Acronym	Explanation	Acronym	Explanation
AI	Artificial Intelligence	SC	Smart Contract
BC	Blockchain	UAV	Unmanned Aerial Vehicle
DApp	Decentralized Application	DT	Digital Twin
FL	Federated Learning	ANN	Artificial Neural Network
IC	Integrated Circuit	LSTM	Long Short-Term Memory
IoT	Internet of Things	RNN	Recurrent Neural Network
ML	Machine Learning	ECC	Elliptic Curve Cryptography
NFT	Non-Fungible Token	GAN	Generative Adversarial Network
PUF	Physically Unclonable Function	SLR	Systematic Literature Review
NLP	Natural Language Processing	CV	Computer Vision
FPGA	Field-Programmable Gate Arrays	CPCS	Cyber-Physical Cloud Systems
IoV	Internet of Vehicles	GPS	Global Positioning System
QR	Quick Response Code	Cobot	Collaborative Robot

2 Background

This section explores the background of blockchain and AI applications in supply chain management and outlines the development landscape of key sectors—ICs, pharmaceuticals, EVs, UAVs, and robotics—as foundational knowledge for this study (see Fig. 4 below).

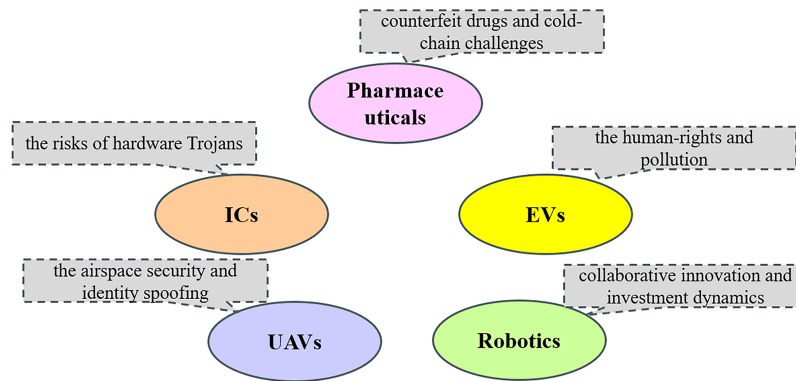


Figure 4: Sector-specific challenges in supply chain traceability

2.1 Blockchain and Supply Chain

Blockchain is a decentralized and distributed ledger technology initially introduced by Satoshi Nakamoto in 2008 [38] to address the trust and anti-counterfeiting challenges associated with Bitcoin. Data immutability is typically guaranteed through cryptographic mechanisms and facilitate consensus among network participants using algorithms such as Proof of Work, Proof of Stake, and Practical Byzantine Fault Tolerance. Although blockchain was originally developed for applications in cryptocurrency, the advancement of smart contracts has significantly broadened its utility. Today, blockchain is increasingly adopted in various diverse sectors, including financial technology, supply chain management, healthcare information systems, and smart manufacturing [39].

In supply chain applications, blockchain offers key advantages such as enhanced transparency, traceability, and non-repudiation. Notable implementations include IBM Food Trust and Walmart’s blockchain-based supply chain tracking systems, which leverage blockchain to enable data integration between companies and source verification. Practical benefits have been realized in areas such as logistics tracking, digital certification, provenance verification of critical products (e.g., diamonds, cocoa, pharmaceuticals), and legal forensics. Meanwhile, blockchain can be integrated with IoT and decentralized storage systems, such as the Inter Planetary File System (abbreviated as IPFS), to strengthen the integrity and credibility of preserved forensic evidence [39].

2.2 AI and Supply Chain

AI, encompassing machine learning (abbreviated as ML), deep learning (abbreviated as DL), natural language processing (abbreviated as NLP), and computer vision (abbreviated as CV), has been widely adopted in supply chain management for a range of functions, including demand forecasting, intelligent scheduling, route optimization, warehouse management, and anomaly detection. Using historical data for predictive modeling, AI enables enterprises to assess supply risks, analyze demand–supply dynamics, and anticipate future trends—thereby facilitating dynamic adjustments to inventory levels and resource allocation [40]. In advancing supply chain transparency, AI can be combined with sensor data and edge computing to support real-time monitoring of production processes and logistics operations. AI-driven analytics can

also identify anomalous supplier behavior, detect fraudulent activities or information obfuscation, and assist in developing risk mitigation strategies. In addition, recent research has introduced Explainable AI (XAI) to enhance the interpretability and trustworthiness of AI-based decisions, particularly in highly regulated environments such as healthcare and finance [41].

2.3 IC and Legal Forensics

ICs are foundational components of modern electronic systems and critical infrastructure, with extensive applications spanning the communications, computing, autonomous vehicles, aerospace, and defense sectors. Due to their strategic importance and high sensitivity, ICs are indeed critical for national security and economic competitiveness. However, global fragmentation of IC design and manufacturing introduces a spectrum of security vulnerabilities [42]:

- (a) Complex supply chain structure: The IC supply chain involves multi-national collaboration across several stages—including front-end design, wafer fabrication, packaging, testing, and system integration. Each stage may involve different vendors, and the lack of verifiable mechanisms at any point may expose the system to exploitation.
- (b) Risk of hardware Trojans: Malicious actors can be embedded in circuits during design or manufacturing processes, which, when triggered under specific conditions, can cause data breaches, system failures, or unauthorized access. These hardware Trojans are notoriously difficult to detect using conventional testing methods, posing severe threats to high-security domains such as defense, finance, and healthcare.
- (c) Challenges in provenance verification and counterfeit detection: Due to the geographically dispersed nature of IC production, issues such as counterfeiting, tampering, and “country-of-origin laundering” are widespread. Addressing these challenges requires robust forensic technologies capable of tracing chip origins and authenticating complete supply histories.

To counter these risks, both academia and industry have invested in a range of countermeasures, including Physical Unclonable Functions (abbreviated as PUF), chip fingerprinting, blockchain-based provenance tracking, and AI-assisted forensic analysis. Collectively, these approaches aim to establish a secure and trustworthy IC supply chain infrastructure that ensures verifiability, resilience, and forensic accountability.

2.4 Pharmaceuticals

The pharmaceutical supply chain is inherently complex and encompasses multiple stages that include raw material procurement, manufacturing, storage, transportation, and distribution. Each stage is subject to stringent regulatory and quality requirements. The industry currently faces several critical challenges [8,9]:

- (a) Counterfeit pharmaceuticals: According to the World Health Organization (abbreviated as WHO), more than 10% of medicines distributed globally are counterfeit, with prevalence even higher in developing countries. These counterfeit drugs may contain incorrect dosages, inactive substances, or harmful ingredients, posing severe risks to public health [10].
- (b) Cold chain logistics management: Many pharmaceuticals—particularly vaccines and biologics—are highly sensitive to temperature fluctuations. They must be transported and stored within tightly controlled thermal ranges. Any deviation can compromise drug efficacy, resulting in financial losses and heightened patient safety concerns.
- (c) Supply disruptions and drug shortages: Globalization of pharmaceutical production has led to increased dependency on specific geographic regions, particularly for active pharmaceutical ingredients, which are often concentrated in a small number of supplier countries. Geopolitical tensions,

natural disasters, and pandemics can rapidly disrupt supply continuity, leading to widespread shortages [12].

To mitigate these challenges, the industry is increasingly investing in advanced logistics management systems, enhancing supply chain transparency, and diversifying sourcing strategies. These efforts aim not only to improve operational resilience but also to safeguard regulatory compliance and protect public health on a global scale.

2.5 EV

The EV industry has witnessed rapid growth in recent years. According to the International Energy Agency, global EV sales are projected to reach 17 million units by 2025, representing more than 20 percent of new vehicle sales [43]. Key trends driving this expansion include the following.

- (a) Sustained market growth: The EV market is expected to increase from USD 396.49 billion in 2024 to USD 620.33 billion by 2030, with a compound annual growth rate of approximately 7.7 percent [3].
- (b) Cost reduction and technological advancement: Improvements in technology and economies of scale are reducing EV production costs and enhancing affordability. At the same time, advances in driving range, charging speed, and intelligent features are expanding the consumer base.
- (c) Policy support and infrastructure development: Governments around the world are promoting the adoption of EV through subsidies, tax incentives, and investments in charging infrastructure, further accelerating market momentum.

This rapid industry transformation is reshaping the automotive sector and has profound implications for energy systems, environmental protection, and urban planning.

2.6 UAV

UAVs have found widespread application in diverse sectors, demonstrating exceptional flexibility and operational efficiency [44]:

- (a) Agricultural management: UAVs enable crop health monitoring, pesticide/fertilizer application, and precision agriculture—contributing to increased yields and optimized resource use.
- (b) Infrastructure inspection: UAVs routinely inspect critical infrastructure—such as transmission lines, bridges, and wind turbines—providing high-resolution imagery while reducing labor demands and enhancing safety.
- (c) Disaster response: In the event of natural disasters like earthquakes and floods, UAVs can quickly survey affected areas, assist in search-and-rescue operations, and enhance situational awareness.
- (d) Environmental protection: UAVs support air quality monitoring, wildlife population surveys, and early detection of forest fires, providing accurate and real-time environmental data.
- (e) Logistics and delivery: UAVs are increasingly being tested and deployed for delivering medical supplies, e-commerce packages, and other small payloads, especially in remote or hard-to-reach regions.

As regulatory frameworks mature and technological advancements—particularly in AI and blockchain—continue to evolve, the potential application domains of UAVs are expected to grow substantially.

2.7 Robotics

Robotic technologies are rapidly advancing and being increasingly adopted in industries such as manufacturing, logistics, and healthcare, positioning them as a fundamental element of Industry 4.0 and automation efforts [45]:

- (a) Collaborative robots: Engineered to work alongside humans, collaborative robots enhance productivity and flexibility—particularly in manufacturing environments with diverse task requirements.
- (b) Humanoid robots: With human-like form and movement, these robots excel in applications requiring adaptability and nuanced interaction, such as caregiving and service roles.
- (c) Specialized robots: Designed for specific functions, including security, firefighting, sanitation, and surveillance patrols.
- (d) Market growth and investment: In the first quarter of 2025, the global robotics sector attracted more than USD 2.26 billion in investment, underscoring strong market interest and high expectations for innovation [46].

With ongoing advancements in AI, sensor technologies, and materials science, robotics is poised to assume an increasingly central role across diverse domains—ultimately becoming a cornerstone of future intelligent and autonomous societies.

3 Survey Methodologies and Taxonomy

This study employs a SLR methodology [47] to investigate the application of AI and blockchain in provenance traceability and forensic verification across the supply chains of ICs, pharmaceuticals, EVs, UAVs, and robotics. The methodological framework comprises data sources, keywords/Boolean logic, inclusion/exclusion criteria, and classification methods.

3.1 Data Sources

The data sources of this survey include:

- (a) IEEE Xplore
- (b) ScienceDirect
- (c) SpringerLink
- (d) ACM Digital Library
- (e) Web of Science
- (f) arXiv

3.2 Keywords and Boolean Logic

To comprehensively map the academic research landscape related to the use of AI and blockchain for provenance traceability and forensic verification within the supply chains of ICs, pharmaceuticals, EVs, UAVs, and robotics, this study employed compound Boolean search queries. The search strategy targeted key themes—such as supply chain traceability, origin authentication, source credibility, risk detection, and intelligent management—through combined keyword logic (see Fig. 5 below):

- (a) IC: (“blockchain” or “artificial intelligence”) and (“supply chain” or “traceability” or “forensic”) and “IC or semiconductor”
- (b) Pharmaceuticals: (“blockchain” or “artificial intelligence”) and (“supply chain” or “traceability” or “forensic”) and “pharmaceutical”
- (c) EV: (“blockchain” or “artificial intelligence”) and (“supply chain” or “traceability” or “forensic”) and (“electric vehicle” or “EV”)
- (d) UAV: (“blockchain” or “artificial intelligence”) and (“supply chain” or “traceability” or “forensic”) and (“UAV” or “drone”)
- (e) Robotics: (“blockchain” or “artificial intelligence”) and (“supply chain” or “traceability” or “forensic”) and “robotics”

Possible Search Strings
(AI or blockchain) and (supply chain or traceability or forensic) and (pharmaceutical or IC or UAV or EV or orobotics)

Figure 5: The compound Boolean logic queries employed in this study for literature retrieval

3.3 Criteria of Inclusion and Exclusion

The inclusion and exclusion criteria for the literature reviewed in this study are defined as follows.

- Inclusion criteria: peer-reviewed journal articles, international conference papers, book chapters, and survey/review studies published from 2016 downwards. In addition, the works address the application of AI and/or blockchain in supply chain management or forensic verification and focus on IC, pharmaceuticals, EV, UAV, or robotics.
- Exclusion criteria: publications that are unrelated to AI, blockchain, the specified industrial sectors (ICs, pharmaceuticals, EVs, UAVs, and robotics), supply chain processes, or forensic applications were omitted from the review.

3.4 Data Processing and Classification Methods

This study adopts a topic-oriented literature review to examine AI and blockchain applications for provenance traceability and forensic verification within the supply chains of ICs, pharmaceuticals, EVs, UAVs, and robotics. We sourced literature from six major databases—IEEE Xplore, ScienceDirect, Springer-Link, ACM Digital Library, Web of Science, and arXiv—using compound Boolean keyword searches. The retrieved records were then filtered through a four-step screening process (see Fig. 6 below):

- Initial Retrieval: Keyword searches across all databases yielded 700 records.
- Title Selection: Title review narrowed the data set to 542 potentially relevant studies.
- Abstract Selection: Abstract reviews excluded low-relevance items, reducing the pool to 254 articles.
- Full-Text Analysis: Detailed examination of abstracts, conclusions, and relevant sections resulted in a final sample of 116 studies for in-depth analysis.

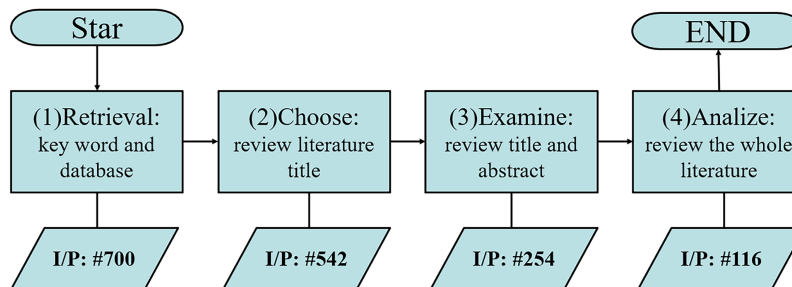


Figure 6: The Process and Criteria of inclusion and exclusion for the literatures of Survey Papers

For clarity and reproducibility, Fig. 7 below presents a baseline schematic diagram summarizing the overall data-processing workflow of this study. It captures the progression from literature retrieval and

screening to thematic classification and synthesis, complementing the detailed selection process already shown in Fig. 6.

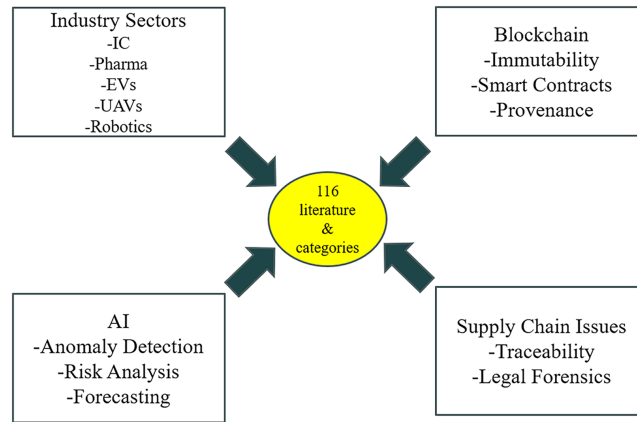


Figure 7: High-level schematic diagram for how the 116 studies be selected and categorized

Although this study does not employ systematic bibliographic analysis, representativeness and relevance are maintained through manual selection and thematic selection (see Table 4 below). A final set of 116 academically significant and application-oriented publications was selected (refer to Section 4), and their content was synthesized to delineate the current landscape of AI and blockchain applications. The selected studies were categorized along three analytical dimensions:

- (a) Application Domain: Industry-specific contexts, including ICs, pharmaceuticals, EVs, UAVs, and robotics.
- (b) Core Technology: AI models (e.g., machine learning, deep learning, and federated learning) and blockchain architectures (e.g., private chains, consortium chains, IPFS, and smart contracts).
- (c) Functional Objective: Targeted outcomes such as supply chain provenance traceability, legal forensic applications, cybersecurity protection, and risk detection.

Table 4: Quality assessment checklist for systematic literature review (SLR Inclusion Criteria)

Inclusion Assessment Questions for SLR Criteria	
1	Does the publication address the application of AI and/or blockchain in supply chain management?
2	Was the publication released after 2016 and classified as a peer-reviewed journal article, international conference paper, book chapter, or survey paper?
3	Does the study explicitly focus on one or more of the following sectors: ICs, pharmaceuticals, EVs, UAVs, and robotics?
4	Is the research related to AI, blockchain, supply chains, traceability, forensic analysis, cybersecurity, IC, pharmaceuticals, EV, UAV, or robotics?
5	Is the paper unrelated to the core themes of supply chains, AI, blockchain, or the five target industries, or does it completely omit traceability-related content?
6	Do the title, abstract, or full text of the publication match the Boolean keyword logic combinations defined in Section 3.2?

(Continued)

Table 4 (continued)

Inclusion Assessment Questions for SLR Criteria	
7	Does the study contribute insights into the integrated technologies, application challenges, or developmental trends of cross-sector traceability systems?

In addition, to highlight the novelty of this study's methodological framework, we emphasize that the classification scheme goes beyond conventional survey structures by introducing a three-dimensional taxonomy that integrates:

- (a) Industry-specific contexts (cross-sector comparison across ICs, pharmaceuticals, EVs, UAVs, and robotics);
- (b) Core technological layers (AI models and blockchain frameworks);
- (c) Functional objectives (traceability, forensic verification, cybersecurity, and risk detection).

This multi-dimensional classification and cross-sector integration, combined with a forensic perspective, differentiates our review from existing surveys and provides a unique contribution to the literature.

4 Blockchain and AI Applications for Provenance Traceability

Geopolitical tensions and trade disputes have increased the importance of traceability of the supply chain. Sensitive electronic products can be hijacked by adversaries during crises for offensive purposes or become national vulnerabilities due to shortages during conflicts [48,49]. In response, the United States has enhanced efforts to combat illegal practices such as country-of-origin laundering, with particular focus on high risk categories including ICs, pharmaceuticals, EVs, UAVs, and robotics. To mitigate long-term security vulnerabilities and prevent tax evasion through falsified origins, deploying technologies such as AI and blockchain is essential to enable provenance tracking and preserve forensic evidence across supply chains (see Fig. 8 below). These technologies not only improve operational efficiency, but also align with national security objectives. Similar efforts are being observed in regions such as the European Union and Japan. The following subsections review current research developments and applications in each of these domains.

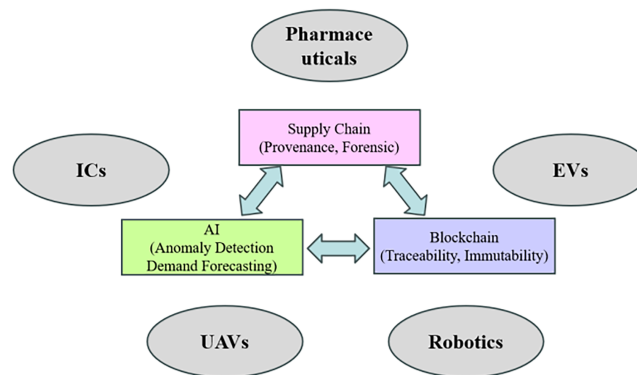


Figure 8: AI + blockchain synergy for supply chain traceability & forensics

4.1 Blockchain, AI, and Supply Chain

4.1.1 Blockchain and AI

Blockchain—a form of decentralized Distributed Ledger Technology—provides immutable, traceable, and tamper resistant record keeping, and has been widely implemented in areas such as supply chain management, IoTs, edge computing, pharmaceutical traceability, communication security, digital identity verification, and legal forensics and evidence preservation [39]. Beyond using cryptographic mechanisms and consensus algorithms to ensure data accuracy, integrity, and transparency, blockchain leverages smart contracts—self-executing agreements embedded in the ledger—to automate operations upon predefined conditions, thereby reducing intermediary costs and minimizing human intervention. This makes blockchain a key technology for building a highly trustworthy digital infrastructure [50].

AI refers to the collective set of technologies that emulate human cognitive behaviors, encompassing ML, DL, NLP, and CV. Trained in large datasets, AI models possess capabilities in classification, recognition, predictive analytics, and automated decision-making. These models are widely applied in various domains—including voice assistants, medical diagnostics, financial, intelligent manufacturing, and smart city—acting as the main drivers of digital transformation and smart infrastructure development [40].

AI is driving digital transformation across industries, and its integration with blockchain technology can enhance system autonomy, trustworthiness, and efficiency [41]. Blockchain offers traceability and anti-counterfeiting to log transactions and promote transparency; however, traditional consensus mechanisms can suffer from inefficiencies. To address this, Ref. [51] introduced a Takagi–Sugeno fuzzy cognitive map–artificial neural network as the inference core of a Traceability Chain Algorithm, significantly accelerating traceability decision-making. In addition, Refs. [52,53] demonstrated that adopting the blockchain Proof of Relationship algorithm as an activation function within neural network models substantially enhances AI's ability to detect maliciously distorted supply-chain information. Moreover, Ref. [54] used ML for inventory allocation in cloud-based supply-chain frameworks, and empirical results show 13%–16% improvement in allocation accuracy over conventional methods. Except the examples noted earlier, further scholarly research and applied studies support the synergistic potential of blockchain and AI [41], including:

- (a) For EV smart-charging networks, blockchain enables decentralized energy trading, reducing operational costs and enhancing trust among stakeholders [36].
- (b) In intelligent vehicular networks, by leveraging blockchain's immutability and anonymization properties, data security is maintained, fostering trustworthy interactions among vehicles, users, and service providers [55].
- (c) For supply chain management, blockchain mitigates the asymmetry between the upstream and downstream information asymmetry information, and AI facilitates predictive analytics of sales data to support automated decision-making [27].
- (d) In the healthcare and pharmaceutical fields, blockchain ensures drug safety and traceability, and AI uncovers latent informational patterns to support drug-related decision-making [34].

In summary, prior studies provide a foundation on the roles of blockchain and AI across supply chain-related domains. Blockchain has been shown to ensure immutability, traceability, and trust through decentralized architectures, while AI contributes predictive analytics, anomaly detection, and decision support across diverse applications. Building on this groundwork, the following section turns specifically to their applications in supply chain traceability.

4.1.2 Blockchain and AI for Supply Chain Traceability

The traceability and transparency of inventory and components have long been critical research topics in supply chain management (see Table 5 below). For example, Ref. [56] investigates warehouse allocation in a dual-warehouse inventory system. Using Markov processes and stochastic arrival models, the study captures real-world demand fluctuations. This dynamic analysis improves forecasting and responsiveness, and integrates replenishment decisions with maintenance services to reduce resource waste. In addition, Ref. [57] examines the management of spare inventory management under supplier disruptions by employing four metaheuristic algorithms—Grey Wolf Optimizer, Genetic Algorithm, Moth Flame Optimization, and Differential Evolution—to identify inventory strategies that minimize total cost. The study suggests that incorporating alternative supply sources can effectively mitigate stockout risks. Additionally, Ref. [58] addresses variability in demand and inventory levels by applying optimization methods based on the Neuts' matrix-geometric approach and Laplace transforms. Performance is evaluated using key inventory metrics such as the average inventory level, repurchase rate, and the service waiting time.

In recent years, increasing social concerns about health, environmental sustainability, human rights, and safety have driven the adoption of emerging technologies—particularly AI and blockchain—in supply chain management. These technologies are being leveraged to enhance component traceability and legal forensics, especially in high-sensitivity industries including the following:

- (a) As the foundational components of all electronic devices, ICs represent a major security vulnerability if embedded with malicious code capable of seizing control during critical operations—an issue with heightened significance amid geopolitical tensions. For instance, the Spanish cybersecurity firm Tarlogic Security reported that Chinese-manufactured ESP32 chips contain undocumented hidden instructions that may serve as backdoors, potentially allowing remote control over millions of IoT devices [7].
- (b) Counterfeit medications were responsible for over 110,000 deaths in the United States alone in 2023 [8], and globally, they contribute to an estimated 1 million deaths annually [9]. In developing countries, one out of every ten medicines are either counterfeit or substandard [10], and up to 30% of pharmaceuticals in regions such as Africa, Asia, and Latin America fail to meet regulatory standards [11]. In response, numerous governments have introduced pharmaceutical traceability regulations to strengthen supply chain transparency [13–15], mandating full end-to-end electronic tracking capabilities within pharmaceutical distribution systems [16].
- (c) Geopolitical conflicts have revealed critical vulnerabilities in global component supply chains, resulting in disruptions in automotive manufacturing activities [17] and posing potential threats to national security. In particular, EV may be exposed to adversarial control, enabling malicious surveillance or attacks. This has raised significant concerns over the transparency and stability of component sourcing. Batteries are the most critical components for EV. However, the extraction and supply of battery raw materials have been repeatedly associated with violations of human rights and environmental degradation [18]. As a result, leading nations have enacted legislation requiring traceability and rigorous oversight of EV components and raw materials to combat fraudulent practices such as origin laundering [19–21].
- (d) The Russia-Ukraine conflict has highlighted the strategic importance of UAVs, which are expected to play a central role in future warfare. However, if UAVs are compromised and remotely controlled by hostile states, they could be transformed into offensive weapons. Similarly, robots are now widely deployed in various supply chain environments. If these systems are embedded with backdoors and activated remotely, they could disable port logistics, sabotage factory production lines, damage healthcare infrastructure, or even target individuals. In response, countries such as the United States,

the European Union, and Japan have introduced legislation to enhance the autonomy of the supply chain and cybersecurity of the robotics industry [22–25]. These regulations are broadly applicable to IoT devices as well.

In addition, food contamination not only poses serious public health risks, but also triggers regulatory mandates requiring end-to-end traceability across all participants in the supply chain [59,60]. When well-established brands experience food safety scandals, consumer trust can be profoundly undermined and may remain difficult to restore even after years of remediation efforts [61]. This erosion of confidence has become a major impetus for corporate investment in traceability technologies powered by AI and blockchain. In this context, Industry 4.0 has emerged as a transformative industrial paradigm that integrates smart manufacturing, digital technologies, and interconnected systems. Therefore, Ref. [62] proposes a traceability system for the food supply chain in the Industry 4.0 framework, integrating IoTs, blockchain, and Advanced DL. The system is built upon LSTM architecture, further enhanced through the incorporation of Gated Recurrent Units and Genetic Algorithms to improve prediction accuracy and model stability. And then Ref. [63] tackles the problem of unauthorized access to private customer data in multi-party sharing environments within Logistics 4.0, presenting a logistics management framework based on Ethereum blockchain and smart contracts. The system adopts RSA asymmetric encryption to ensure data confidentiality and system integrity, and demonstrates its effectiveness in safeguarding logistics processes and customer information against cyber threats. In addition, Ref. [64] investigates fault diagnosis in industrial equipment within the cloud-based IOT architectures of Industry 4.0 and 5.0. By employing an LSTM deep learning model, the study enhances the decision-making abilities of digital twins in identifying failure patterns and technical diagnostics, with the proposed approach validated through simulation and real-world datasets.

Table 5: A relative comparison of approaches used to apply AI and blockchain in supply chain traceability and forensic contexts

Authors/Year	Objective	Approach	Technology	1	2	3	4	5
Barron (2023) [56]	Integrate replenishment and maintenance in stochastic inventory system	Markov model, stochastic inventory simulation	Inventory systems, logistics	Y	N	Y	N	N
Baghizadeh et al. (2023) [57]	Reduce supplier disruption risk using metaheuristics	GWO, GA, MFO, DE metaheuristic algorithms	Supplier risk modeling	Y	N	Y	N	N
Harikrishnan et al. (2022) [58]	Optimize queue-based inventory system with optional retrieval	Matrix geometric method, Laplace transform	Stochastic inventory	N	N	Y	N	N
Khan et al. (2020) [62]	Optimized food provenance system in Industry 4.0	IoT + blockchain + deep learning (LSTM, GRU, GA)	Sensors, DL models	Y	Y	Y	Y	N

(Continued)

Table 5 (continued)

Authors/Year	Objective	Approach	Technology	1	2	3	4	5
Nwosu et al. (2022) [63]	Protect logistics data from unauthorized access	Blockchain with RSA asymmetric encryption	RSA, Ethereum, smart contracts	N	Y	Y	N	N
Rodriguez-Aguilar et al. (2024) [64]	Fault diagnosis of actuators using digital twin and DL	LSTM-based DL for fault detection	Digital twin, IIoT, LSTM	Y	N	N	N	N
Tian (2016) [65]	Enable traceability in agri-food supply chain using RFID and blockchain	RFID + blockchain system	RFID, blockchain	N	Y	Y	Y	N
Monteiro et al. (2021) [66]	Track agrochemical usage and trading	IoT + machine learning + blockchain	Sensors, RFID, blockchain	Y	Y	Y	Y	N
Shahbazi et al. (2021) [67]	Prevent fraud in perishable food chains	Blockchain + machine learning + fuzzy logic	BMLFITS framework	Y	Y	Y	Y	N
Sun et al. (2023) [68]	Pricing strategy in blockchain-enhanced agri SC	Game theory modeling	Consumer behavior modeling	N	Y	Y	Y	N
Chen et al. (2021) [69]	Optimize agri-food SC with dynamic decision system	Deep reinforcement learning + blockchain	DRL, smart contracts	Y	Y	Y	N	N
Tian et al. (2023) [70]	Vessel selection in a limited choice environment	Random forest models for decision support	Maritime logistics, ML	Y	N	Y	N	N
Bamakan et al. (2021) [71]	Evaluate service SC performance	Blockchain + Di-ANFIS + IoT	Fuzzy inference system	Y	Y	Y	N	N
Chidepatil et al. (2020) [72]	Improve plastic waste economy through AI + blockchain	Multi-sensor fusion + blockchain	AI, sensors, blockchain	Y	Y	Y	N	N
Dey et al. (2022) [73]	Quantify and reduce food waste	SmartNoshWaste framework with blockchain, QR, RL	Blockchain, ML, QR	Y	Y	Y	Y	N

(Continued)

Table 5 (continued)

Authors/Year	Objective	Approach	Technology	1	2	3	4	5
Kamble et al. (2022) [74]	Implement a digital twin in sustainable manufacturing	IoT + blockchain + cloud	Digital twin, cloud, IoT	N	Y	Y	N	N
Wong et al. (2021) [75]	Real-time maritime SC risk management	Blockchain + machine learning + cloud	Supply chain monitoring	Y	Y	Y	N	N
Ivanov (2019) [76]	Investigate the impact of digital technologies and Industry 4.0 on the ripple effect and supply chain risk analytics	Review of the literature and development of conceptual frameworks	Big data analytics, blockchain, Industry 4.0, advanced tracking systems, additive manufacturing	Y	Y	Y	Y	N
Rodríguez-Espíndola (2020) [77]	Explore integration of emerging technologies in humanitarian supply chains	Case study and conceptual framework	AI, blockchain, 3D printing	Y	Y	Y	N	N

Note: 1: AI involved, 2: Blockchain involved, 3: Supply chain involved, 4: Traceability involved, 5: Forensic involved.

In the area of Radio Frequency Identification (abbreviated as RFID), Ref. [65] proposed a food supply chain traceability system that integrates RFID with blockchain to allow the collection and sharing of authentic data at all stages of the supply chain—from agricultural production to storage, distribution, and retail. The system improves food safety and transparency. Likewise, Ref. [66] integrated sensors, microcontrollers, RFID, ML, and blockchain to develop the Agrochemical Pervasive Traceability Model, which is designed to monitor the use, recycling, and trading of agrochemicals. This model addresses pesticide misuse, environmental pollution, and illegal distribution.

For agriculture, Ref. [67] proposed a food traceability system for perishable supply chains by integrating blockchain, ML, and fuzzy logic to prevent shelf-life manipulation and product data falsification. In addition, Ref. [68] applied game theory to investigate the factors influencing consumer preferences for traceability in fresh agricultural products. Then a pricing decision model was developed to help firms implement blockchain under competitive market conditions, enabling optimal pricing and profit maximization. Furthermore, Ref. [69] introduced a framework that combines blockchain with deep reinforcement learning to dynamically adjust agricultural goods production and storage in response to market demand and cost fluctuations, thus improving overall profitability.

In logistics and service, Ref. [70] examined the selection of vessels within logistics management. Faced with limited shipping options, the study used the Random Forest algorithm to develop multiple predictive models to optimize vessel selection strategies. The goal was to avoid potentially non-compliant

ships and, in turn, enhance the efficiency of Port State Control inspections and improve maritime safety. In addition, Ref. [71] proposed a decentralized intelligent diagnostic and evaluation framework with integrating blockchain, neuro-fuzzy, and IoT. This framework supports performance assessment and forecasting within service supply chains, ultimately fostering greater transparency and trust among stakeholders.

For sustainability and circular economy, Ref. [72] developed a plastic classification system by integrating blockchain-based smart contracts with multi-sensor AI data fusion algorithms. The system supports the exchange of information between sorting facilities, recycling companies, and manufacturers, thus improving the transparency and precision of plastic waste classification. In addition, Ref. [73] introduced the Smart-NoshWaste framework, which combines blockchain, cloud computing, QR code, and reinforcement learning to quantify food waste, resulting in a 9.46% reduction in food waste. To add further, Ref. [74] highlighted that the integration of IoT, cloud computing, and blockchain within a digital twin system—linking physical and virtual environments—can enable high-quality, rapid, and customized smart manufacturing supply chains across sectors. These innovations ultimately improve operational performance and contribute to broader sustainability objectives.

For disruption risk, Ref. [75] proposed an integrated architecture that combines blockchain, ML, and cloud computing to meet the increasing demand for immutable transaction records. The framework demonstrates real-time detection and decision-making capabilities in maritime risk management. In addition, Ref. [76] developed a supply chain risk analysis framework that emphasizes the importance of digital transformation in enhancing the predictive capacity for disruption risks, while also highlighting the potential of cyber-physical supply chains in mitigating such risks. Not only that, Ref. [77] introduced a comprehensive framework that integrates blockchain, AI, and 3D printing to enhance the effectiveness of humanitarian supply chains during large-scale disaster events, supported by in-depth analysis of empirical cases.

4.2 IC Traceability and Forensics

ICs are the foundational components of all electronic industries. However, the increasing globalization and fragmentation of the semiconductor design and manufacturing sectors over the past two decades have significantly intensified hardware security concerns. Infiltration of counterfeit electronic components into the supply chain has resulted in failures of critical infrastructure and financial losses for end-users of essential systems, which presents a widespread global challenge [42]. In the same manner, the common practice of outsourcing chip fabrication by IC design firms has exposed supply chains to hardware Trojan threats [7]. In response, IC traceability and forensic technologies have emerged as vital research areas, with the aim at tracking the origin and distribution of chips and to prevent illicit activities such as origin laundering and tax evasion—thereby reinforcing the integrity of the supply chain and supporting national security efforts (see Fig. 9 below).

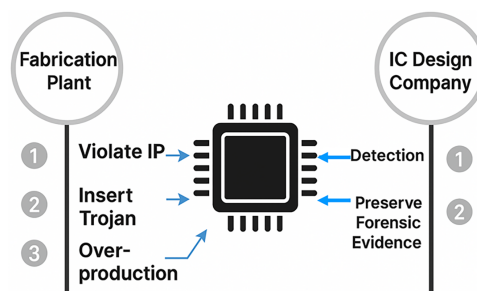


Figure 9: The Blockchain-based Forensic Procedure for fragmentation of IC design and manufacturing sectors

4.2.1 IC Traceability and Legal Forensics

Blockchain is increasingly adopted to enhance IC traceability and the preservation of forensic evidence, owing to its inherent features of immutability, decentralization, and transparency. Meanwhile, AI is leveraged to improve supply chain efficiency and to track carbon footprints (see Table 6 below). According to [42], the infiltration of counterfeit IC into the supply chain has become a global challenge. Most existing blockchain-based traceability methods focus on post-sale tracking—that is, after IC design companies deliver chips to customers. However, before chips are shipped, traceability becomes more complex due to the involvement of multiple foundries. To address this issue, the study proposes a comprehensive IC traceability framework that spans the entire process, from manufacturing and testing to sales. This enables IC design firms to precisely monitor chip origin and distribution, thereby enhancing supply chain transparency and resistance to counterfeiting. Furthermore, Ref. [78] investigated the risks of counterfeiting and tampering in the increasingly globalized IC supply chain, noting that current methods often fail to effectively verify the true origin of chips. To overcome this limitation, the study introduced a forensic identification circuit, which utilizes intrinsic process variations within ICs to identify and trace their manufacturing origins. For experimental validation, the researchers fabricated 159 ICs incorporating three different circuit types. The proposed method achieved identification accuracy rates of up to 98% for both foundry recognition and production batch identification.

Table 6: A relative comparison of approaches used to apply AI and blockchain in supply chain traceability and forensic contexts of IC industry

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Rekha et al. (2021) [42]	End-to-end IC traceability	Blockchain-based traceability framework	Blockchain	N	Y	Y	Y	Y
Helinski et al. (2016) [78]	Manufacturer attribution using IC variations	FORAB forensic method	Forensic circuits	N	N	Y	Y	Y
Bloom et al. (2010) [79]	Prevent tampering during IC fab	TPM tracking of design phases	TPM	N	N	Y	Y	Y
Shandilya et al. (2025) [80]	Zero-trust IC validation architecture	SPDM chip-to-chip certificate auth	Zero trust, verification	Y	Y	Y	N	N
Kulkarni et al. (2019) [81]	Track IC tampering in supply chain	Blockchain & smart contracts	Blockchain, supply chain sim.	N	Y	Y	Y	Y
Dangi et al. (2024) [82]	Detect ransomware via memory forensics	ML-enabled forensic memory analysis	ML, volatile memory forensics	Y	N	Y	N	Y
Kulkarni et al. (2023) [83]	Secure FPGA post-fab validation	Blockchain + Ring Oscillator PUF	Blockchain + Ring Oscillator PUF	N	Y	Y	Y	Y

(Continued)

Table 6 (continued)

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Kulkarni et al. (2024) [84]	Zero-trust FPGA security	Blockchain + Ring Oscillator PUF	Blockchain + Ring Oscillator PUF	N	Y	Y	Y	Y
Khan et al. (2021) [85]	Secure multimedia forensic chain of custody	Hyperledger Sawtooth + blockchain	Blockchain	N	Y	Y	Y	Y
Ab Rahman et al. (2016) [86]	Embed forensic design in cloud-based systems	Forensic-by-design	Forensic architecture	N	N	Y	N	Y
Nelufule et al. (2024) [87]	Digital forensics in Industry 4.0/5.0	Adaptive forensic framework	IoT, multi-agency coordination	N	N	Y	N	Y
Dave (2022) [88]	Secure forensic data in IoT	PUF + lightweight encryption	IoT, forensics	N	N	Y	N	Y
Sonawane et al. (2024) [89]	Forensic Apps for report delivery	Ganache + smart contracts	Blockchain, Ethereum	N	Y	N	Y	Y
Patil et al. (2021) [90]	Evidence protection via blockchain	Immutable forensic report tracking	Blockchain	N	Y	N	Y	Y
Sangekar et al. (2024) [91]	Secure lifecycle of forensic data	Smart contract + encryption	Blockchain, forensics	N	Y	N	Y	Y
Yap et al. (2024) [92]	AI for extracting IC contract clauses	CUAD-RoBERTa + PERFECT framework	NLP, AI	Y	N	Y	N	N
Tassel et al. (2023) [93]	Semiconductor fab scheduling using AI	Self-supervised + reinforcement learning	AI, semiconductor scheduling	Y	N	Y	N	N

Note: 1: AI involved, 2: Blockchain involved, 3: Supply chain involved, 4: Traceability involved, 5: Forensic involved.

For IP infringement and malicious modifications, when chip fabrication is outsourced, IC design companies must submit confidential GDS-II layout files, which introduces risks of IP tampering, theft, and counterfeiting. To mitigate these risks, Ref. [79] proposed a forensic mechanism based on the Trusted Platform Module that records changes and operations across three stages in the foundry: GDS-II editing, mask conversion, and mask printing. This mechanism ensures full traceability throughout the process. In IC design, companies can later extract these records from the physical chip and compare them with the original manufacturing process to verify whether unauthorized modifications, duplications, or overproduction has occurred. These records can also serve as legal evidence for prosecution and counterfeit traceability. In addition to that, Ref. [80] introduced a certificate-based Security Protocol and Data Model to establish a “chip-to-chip” authentication framework. Adhering to the zero-trust principle, every chip must undergo verification prior to deployment to ensure authenticity and provenance. Similarly, Ref. [81] examined the

security vulnerabilities introduced by globalization of the IC supply chain, such as counterfeit chips and insertion of hardware Trojans. The study proposed a framework enabled by blockchain and smart contract to monitor chip integrity during both manufacturing and transportation. At each stage, relevant parameters and test results are logged, and each participant independently updates the blockchain. In the event of malicious activity, the system can precisely identify the stage and responsible party through timestamped records and change logs, thereby providing reliable forensic evidence. The feasibility of this approach was validated using a simulated supply chain network built on the IBM platform.

With respect to memory forensics, semiconductor manufacturing functions as a highly automated supply chain system that integrates ML, sensors, UAVs, and big data. While improving efficiency, these technologies increase the risks of ransomware and fileless malware attacks. Sensitive data are often stored in volatile memory, which is lost upon system shutdown, making it difficult for forensic investigators to determine the nature of the attack or identify the specific type of malicious software involved. To address this challenge, Ref. [82] proposed a Live Memory Forensics approach that enables the extraction and analysis of volatile memory in real-time. ML is incorporated to enhance both the efficiency and accuracy of the memory acquisition and analysis.

4.2.2 FPGA Traceability and Legal Forensics

With the growing demand for field-programmable gate arrays (abbreviated as FPGA) across various sectors, counterfeit and recycled FPGA chips have increasingly infiltrated supply chains, posing risks to critical infrastructure and raising concerns about hardware Trojans. To address these threats, Ref. [83] proposed a security method that integrates PUF with blockchain to strengthen verification mechanisms in the downstream FPGA supply chain. The method was simulated using the Ganache framework provided by the Truffle suite, demonstrating its effectiveness in authenticating the integrity of the FPGA and tracking.

In the same way, to counter threats such as intellectual property theft, counterfeiting, and bitstream tampering that undermine the trustworthiness of FPGA, Ref. [84] introduced a zero-trust architecture that combines blockchain with PUF based on ring oscillator. Using the Artix-7 Xilinx FPGA as a test case, the framework was evaluated through a series of targeted attack scenarios aligned with zero-trust principles. The experimental results confirmed its effectiveness in mitigating potential security breaches.

Together, these studies highlight the growing importance of blockchain-integrated hardware security frameworks in ensuring the authenticity, traceability, and resilience of programmable logic devices within global supply chains.

4.2.3 Blockchain and Legal Forensics in Supply Chains

The exchange of multimedia data over the Internet often involves multiple institutions that share, modify, and reuse information, which can compromise the integrity, reliability, and credibility of digital forensic investigations. To address this issue, Ref. [85] proposed the MF-Ledger blockchain framework based on Hyperledger Sawtooth. This architecture enables digital forensic processes to record protocols and evidence securely within a private network, using encrypted private blockchain ledgers to prevent evidence tampering. By the same token, as supply chain operations increasingly migrate to cloud environments, cyber-physical cloud systems (abbreviated as CPCS) are exposed to elevated risks of cyberattacks. In response, Ref. [86] examined the security challenges posed by threats related to CPCS and emphasized the importance of incorporating a forensic design approach during the development phase of the system.

With the advent of Industry 4.0 and Industry 5.0, the increasing complexity of emerging technologies and data environments in supply chain IoT systems has introduced significant challenges to digital forensics.

To mitigate these risks, Ref. [87] proposed an adaptive digital forensic framework that incorporates cross-border judicial collaboration and integration of industrial system. This framework brings together dynamic evidence collection techniques, advanced data analytics tools, and multi-stakeholder cooperation mechanisms to ensure the integrity, reliability, and admissibility of forensic evidence. In the same way, IoT devices used in supply chain management are typically resource-constrained, limiting their capacity to support advanced cybersecurity mechanisms. As a result, they are highly susceptible to threats such as Trojans, malicious code, and reverse engineering. Therefore, Ref. [88] implemented lightweight cryptographic techniques in conjunction with PUF to enhance device-level protection and secure data essential for IoT forensics. This approach contributes to faster, and more accurate cybercrime investigations.

For the preservation of forensic evidence, Ref. [85] emphasized that modern criminal investigations are highly dependent on the secure management of forensic evidence, which requires both robust storage mechanisms and comprehensive documentation throughout the evidence transfer process. To address this challenge, Ref. [89] utilized Ganache developed by Truffle Suite to build a private Ethereum blockchain environment to rapidly deploy smart contracts and DApp. This environment was used to simulate the multi-stage transmission of forensic reports within the forensic evidence chain. Similarly, traditional methods of transmitting forensic evidence—such as physical delivery or email—are vulnerable to tampering, which can jeopardize the integrity of the court. To address these threats, Ref. [90] proposed a blockchain-based solution on the Ethereum platform to establish an immutable and traceable digital forensic reporting system. This system improves transparency and ensures high-integrity handling of forensic data throughout criminal investigations. Consequently, Ref. [91] introduced a new blockchain-enabled forensic preservation framework that integrates cryptographic mechanisms with smart contracts to support transparent, secure, and verifiable lifecycle management of forensic evidence.

4.2.4 Blockchain and Legal Forensics in Supply Chains

Companies such as Microsoft and Infineon frequently need to identify critical clauses—such as delivery deadlines, warranty periods, and payment terms—within long IC supply contracts. Traditionally, this task has relied on manual processes that are time-consuming and error-prone. To improve efficiency, Ref. [92] proposed the use of a pre-trained language model CUAD-RoBERTa in combination with the PERFECT few-shot learning framework to improve the accuracy and speed of contract clause extraction. The model was trained and validated using 138 contracts signed by Infineon since 1990, demonstrating consistent F1-score performance across diverse clause types.

Inclusion, Ref. [93] introduced a semiconductor process scheduling method that integrates self-supervised learning with reinforcement learning. This approach addresses the complex, continuous, stochastic, and dynamic nature of modern semiconductor manufacturing scheduling challenges. The results indicate a significant reduction in order delays and completion times, along with a more efficient allocation of processing resources.

4.3 Pharmaceuticals

Approximately one million people die each year due to counterfeit medications [9], and up to 30% of pharmaceutical products in regions such as Africa, Asia, and Latin America fail to meet regulatory standards [11]. This widespread issue is largely attributed to the complexity and fragmentation of the pharmaceutical supply chain, where illicit practices such as origin laundering hinder transparency and make traceability highly challenging. To address these issues, an intelligent pharmaceutical supply chain system that integrates blockchain's immutability with AI's analytical and predictive capabilities is needed to ensure verifiability, transparency, and traceability [94]. In much the same way, Drug shortages can also trigger social

unrest, prompting many governments to implement pharmaceutical traceability regulations [13–15]. These laws require comprehensive, end-to-end electronic traceability throughout the supply chain [16], creating a favorable environment for the adoption of blockchain and AI in pharmaceutical supply chain management (see Table 7 below).

Table 7: A relative comparison of approaches used to apply AI and blockchain in supply chain traceability and forensic contexts in pharmaceutical industry

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Kaur (2021) [94]	Survey applications of AI, blockchain, and big data in the medical and global health domains	Systematic literature review and data analysis	AI/ML, Big Data, Blockchain	Y	Y	Y	N	N
Subbarao et al. (2024) [95]	Monitor raw materials and drug flow in supply chain using private blockchain	Hyperledger Fabric supply chain traceability system	Hyperledger Fabric	N	Y	Y	Y	N
Kumar et al. (2019) [96]	Detect counterfeit drugs early via encrypted QR and blockchain	Blockchain + QR code traceability	Blockchain, QR	N	Y	Y	Y	N
Kulkarni et al. (2024) [97]	AI + blockchain drug traceability platform with QR-coded tracking	AI analytics + blockchain ledger	Blockchain, QR, AI	Y	Y	Y	Y	N
Abbas et al. (2020) [10]	Drug supply chain management and recommendation using ML + blockchain	N-gram + LightGBM model + blockchain API integration	Blockchain, ML	Y	Y	Y	Y	N
D'souza S et al. (2021) [98]	Decentralised DApp system for counterfeit drug tracking	Ganache + Web3.js + smart contracts + AI chatbot	Blockchain, AI	Y	Y	Y	Y	N
Ghadge et al. (2022) [99]	Conceptual framework for blockchain implementation in pharma supply chains	Review + conceptual framework	Blockchain	N	Y	Y	Y	N

(Continued)

Table 7 (continued)

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Kuruvilla et al. (2023) [100]	Industry 4.0 framework for pharma SCM with AI demand prediction and blockchain traceability	IoT monitoring + AI-based forecasting + blockchain	Blockchain, IoT, AI	Y	Y	Y	Y	N
Silva-Aravena et al. (2020) [101]	Dynamic decision tool for hospital pharmacy inventory	Mathematical inventory optimization	SCM tools	N	N	Y	N	N
Charles et al. (2023) [27]	Systematic review of blockchain + AI integration in supply chain	Literature analysis	Blockchain, AI	Y	Y	Y	Y	N
Zhang et al. (2021) [102]	Pharmaceutical cold chain management combining DL & blockchain	Deep learning prediction + IoT + blockchain	Deep learning, IoT, Blockchain	Y	Y	Y	Y	N
Arora et al. (2025) [103]	Blockchain-integrated IoT system for cold chain monitoring of pharmaceuticals	IoT data recording + smart contracts	IoT, Blockchain	N	Y	Y	Y	N
Josy et al. (2024) [104]	Improve cold chain vaccine preservation and inventory efficiency using smart technologies	System design and implementation review	IoT, Blockchain, AI-based predictive analytics	Y	Y	Y	Y	N
Shanthi et al. (2023) [105]	Blockchain + ML optimized drug supply management	Hyperledger Fabric + GBDT + AOA	Blockchain, ML	Y	Y	Y	Y	N
Jamil F et al. (2019) [11]	Hyperledger Fabric-based smart hospital drug tracking system	Smart contract implementation	Blockchain	N	Y	Y	Y	N

(Continued)

Table 7 (continued)

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Anu et al. (2024) [106]	Authentication and blockchain-based record for drug supply chain	Blockchain + cryptographic authentication	Blockchain	N	Y	Y	Y	N
Gupta et al. (2021) [107]	Propose a secure and intelligent telesurgery system using blockchain, AI, and UAVs	System architecture design and algorithm implementation	AI (XGBoost), blockchain, UAVs, IPFS, 6G	Y	Y	Y	Y	N
Ahalawat et al. (2025) [108]	Bibliometric review of e-pharmacy tech including AI and blockchain	Bibliometric analysis	Blockchain, AI	Y	Y	Y	Y	N
Mondal et al. (2024) [109]	AI-driven federated & blockchain approach for personalized medicine	FL + blockchain + quantum computing	Blockchain, AI	Y	Y	Y	Y	N
Pisirgen et al. (2025) [110]	Review of digital twin with AI and blockchain in precision medicine	Systematic review of DT + blockchain	Blockchain, AI, Digital Twin	Y	Y	Y	N	N

Note: 1: AI involved, 2: Blockchain involved, 3: Supply chain involved, 4: Traceability involved, 5: Forensic involved.

4.3.1 AI and Blockchain Applications in Pharmaceutical Traceability

Hyperledger Fabric is a private enterprise blockchain platform developed under the Linux Foundation. Based on this framework, Ref. [95] designed a blockchain system capable of continuously monitoring and tracking the origins of raw materials and the distribution of pharmaceutical products throughout the supply chain, thus enhancing traceability and anti-counterfeiting capabilities. The system has been tested and validated for feasibility and effectiveness.

A core challenge in combating counterfeit drugs lies in the inability to verify the authenticity of raw materials in the early stages of pharmaceutical production. Therefore, Ref. [96] proposed a mechanism that combines blockchain with encrypted QR codes to improve the verification of the authenticity of ingredients during manufacturing, strengthening the detection of counterfeit drugs. In addition to that, Ref. [97] introduced an integrated traceability and anti-counterfeiting framework for the pharmaceutical supply chain that leverages both blockchain and AI. In this system, all pharmaceutical items are registered on the blockchain from the raw material stage and are assigned unique QR codes to record and retrieve complete

distribution histories, allowing identification of counterfeit sources. AI is also used to analyze certification documents and laboratory test reports, improving the credibility and reliability of the supply chain.

For the widespread distribution of counterfeit and substandard pharmaceuticals, Ref. [10] proposed an integrated blockchain and ML system to enable the complete tracking of raw material sources and the drug distribution pathways. It incorporates an N-gram model combined with Light Gradient Boosting Machine to train a pharmaceutical recommendation model. The model was developed and validated using data from Irvine Machine Learning Repository of the University of California, and integrated into a blockchain framework via a Representational State Transfer Application Programming Interface. Building on similar objectives, Ref. [98] developed a blockchain–AI hybrid system with all components deployed on a local Ganache blockchain. Integration with Truffle was achieved using Web3.js. The DApp was built using the React framework. The mobile frontend was developed using Flutter and a Rasa-based chatbot supported interactive communication. Smart contracts were used to ensure verifiability and traceability for all transactions within the supply chain, providing an effective mechanism to identify and investigate counterfeit pharmaceutical circulation. Furthermore, Ref. [99] reviewed recent studies on key challenges in traditional pharmaceutical supply chains—including drug counterfeiting, product recalls, patient privacy, and clinical trials. The study underscored the potential of blockchain to improve transparency and information reliability, thereby strengthening the authenticity of pharmaceutical products and curbing the spread of counterfeit drugs.

Industry 4.0 is a concept of cross-technological integration that extends beyond AI and robotics to encompass a comprehensive intelligent supply chain platform incorporating AI, blockchain, IoT, and big data analytics. This integrated architecture not only enhances the intelligence and automation of healthcare supply chains but also enables effective pharmaceutical inventory management. In this context, Ref. [100] proposed an Industry 4.0–based framework that applies blockchain to trace the origins of raw materials and the distribution routes of pharmaceutical products, thus preventing counterfeit drugs from infiltrating the supply chain. AI models are also utilized to forecast pharmaceutical demand and mitigate risks of shortages or overstocking, while Industrial IoT is used to monitor drug storage conditions and enhance procurement transparency. In addition to that, Ref. [101] developed an algorithmic decision support tool geared for pharmacy inventory management. This tool optimizes the procurement and storage planning of pharmaceutical products. Empirical validation showed that the proposed approach reduces costs by more than 7% compared to traditional methods and provides more effective maintenance of critical drug inventories.

4.3.2 AI and Blockchain Applications in SCM

In logistics and cold chain management, Ref. [27] conducted a systematic review of existing studies on the integration of blockchain and AI in supply chain applications. The review highlighted that these technologies contribute to improved supply chain stability and operational efficiency, accelerate logistics processes, reduce costs, and improve both information transparency and traceability of product origins. Given that pharmaceutical cold chains involve significantly higher storage and transportation costs, the need for accurate demand forecasting becomes critical for cost control. Addressing this, Ref. [102] developed a deep learning–based model to predict demand for cold chain pharmaceuticals and integrated blockchain, cloud storage, and IoT to track supply chain activities, thus improving transparency and quality assurance. Not only that, Ref. [103] proposed a system that integrates blockchain with IoT-based environmental sensors to monitor and log real-time temperature and humidity data throughout the cold chain logistics process. This approach ensures the safety and integrity of temperature-sensitive pharmaceutical products. Using the immutability of blockchain and the automated execution of smart contracts, the system improves both

transparency and trust throughout the pharmaceutical cold chain. In a similar manner, conventional vaccine tracking methods are often inefficient and prone to spoilage. To address this challenge, Ref. [104] introduced a cold chain storage solution incorporating IoT technology, capable of issuing real-time alerts when vaccine inventory is low or nears expiration. The system can also be integrated with cloud platforms and AI-driven forecasting models to further optimize vaccine storage and management.

Regarding Hyperledger Fabric, Ref. [105] proposed a pharmaceutical supply chain management approach that integrates blockchain with ML to achieve traceability of drug distribution. The system is developed on the Hyperledger Fabric framework and employs Gradient Boosting Decision Trees to generate drug recommendations. To optimize model performance, the Archimedes Optimization Algorithm is used for hyperparameter tuning. Experimental validation using a standard dataset demonstrated high effectiveness in multiple evaluation metrics. Equally important, Ref. [11] implemented a blockchain-based pharmaceutical supply chain platform built on the Hyperledger Fabric architecture. Smart contracts are deployed to enable authorized access to electronic drug records, ensuring data immutability and improving system transparency. Performance evaluation using Hyperledger Caliper confirmed the efficiency of the platform in terms of transaction throughput, latency, and resource utilization. To build on this, Ref. [106] introduced a blockchain architecture that incorporates an authentication mechanism to document the entire life cycle of pharmaceuticals—from the sourcing of raw materials through manufacturing, storage and distribution. The system balances transparency with the protection of sensitive information and enables users to verify records through unique identifiers and cryptographic techniques. Any anomalies detected in the data may signal the presence of counterfeit drugs.

For last-mile delivery of pharmaceuticals, Ref. [107] proposed the Blockchain and AI-empowered Telesurgery System for 6G, which integrates UAVs to establish temporary and rapid pharmaceutical logistics networks. This system addresses transportation bottlenecks in emergency medical scenarios by enabling efficient and timely delivery of critical medications. Currently, Ref. [108] examined trends in technological adoption in the online pharmacy sector and identified the integration of emerging technologies—particularly AI and blockchain—as a critical driver of innovation. These technologies are transforming both the technical capabilities and the managerial models of online pharmaceutical services, fostering greater efficiency, transparency, and responsiveness within digital healthcare ecosystems.

4.3.3 Blockchain and Federated Learning

Federated learning has rapidly emerged as a prominent research domain in recent years. Ref. [109] proposed an integrated architecture that combines AI-driven federated learning, blockchain, and quantum computing to enhance data privacy protection, facilitate real-time analytics, and share secure patient data between distributed nodes. This approach supports improved diagnostic accuracy, more efficient treatment planning, and improved disease prediction in healthcare settings. Simultaneously, Ref. [110] examined the application of federated ML within digital twin systems, emphasizing the prevalent use of hybrid algorithms that blend supervised and unsupervised learning to improve the accuracy and performance of the digital twin. The study also further observed that integrating blockchain with generative AI can enhance both the functionality and data security of digital twin platforms.

4.4 EVs

With the rapid development of EVs, related supply chain challenges have attracted increasing attention. Disruptions in component supply can stop vehicle production [17], and EVs can be compromised for surveillance or attacks. In the meantime, sourcing the procurement of battery raw materials has been implicated in human rights abuses and environmental pollution [18], prompting major countries to legislate

traceability and strict regulation of EV components and raw materials to prevent activities such as origin laundering and falsified provenance [19–21]. Consequently, emerging technologies such as blockchain and AI are applied to EV supply chains (see Table 8 below) to improve transparency, prevent counterfeiting, reduce environmental impact, support sustainability goals and ensure compliance with international regulations. For example, Ref. [111] highlighted blockchain's immutability, transparency, traceability, and decentralization as key enablers to improve the security and credibility of EV-related data. Current research has identified three main application areas:

- (a) EV charging infrastructure: Blockchain facilitates recording and validation of charging transactions to ensure transaction transparency and prevent fraudulent behaviors.
- (b) Battery supply chains: Blockchain allows tracking of material provenance and distribution flows, improving component traceability and compliance with sustainability policies.
- (c) Vehicle connectivity: Blockchain integration supports demand-response management and enhances data privacy

Table 8: A relative comparison of approaches used to apply AI and blockchain in supply chain traceability and forensic contexts in EV industry

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Rana et al. (2024) [111]	Secure EV charging, energy management, supply chain transparency	Blockchain-based ledger for charging and energy management	Blockchain, supply chain	N	Y	Y	Y	N
Chen et al. (2024) [112]	Theoretical blockchain ecosystem for lithium-ion battery traceability	Conceptual framework for battery sourcing	Blockchain	N	Y	Y	Y	N
Gohil et al. (2023) [113]	Detect malicious parts, trace EV component origins	ANN/LSTM/RNN + smart contracts	ML, blockchain	Y	Y	Y	Y	N
Mugurusi et al. (2022) [114]	Trace cobalt from ASM mining for cobalt sustainability	Blockchain-based provenance for cobalt mining	Blockchain	N	Y	Y	Y	N
Wessel et al. (2023) [115]	Laser-etched QR traceability in battery cell production	QR + traceability system + blockchain + AI defect detection	Blockchain, AI	Y	Y	Y	Y	N
Rufino Júnior et al. (2022) [116]	Review blockchain in battery supply chain, traceability & transparency	Systematic review	Blockchain	N	Y	Y	Y	N

(Continued)

Table 8 (continued)

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Ribeiro da Silva et al. (2023) [117]	Use blockchain & DTP for battery lifecycle management	Digital Battery Passport on blockchain	Blockchain	N	Y	Y	Y	N
Choudhary et al. (2024) [118]	QR-coded battery tracking & recycling with AI analytics	QR + blockchain + AI anomaly detection	Blockchain, AI	Y	Y	Y	Y	N
Bragadeesh et al. (2022) [119]	Lifecycle tracking of vehicles using ML + smart contracts	Blockchain + ML + fuzzy logic	Blockchain, ML	Y	Y	Y	Y	N
Arunmozhi et al. (2022) [120]	Blockchain + AI for autonomous vehicle supply chains	Smart contracts + ML performance metrics	Blockchain, AI	Y	Y	Y	Y	N
Cheng et al. (2024) [121]	Use LLM + GCN for EV battery supply chain disruption prediction	SHIELD predictive analytics	AI, blockchain	Y	Y	Y	Y	N
Banerjee et al. (2024) [122]	AI for SCM in auto industry	Mixed ML & IoT analysis	AI	Y	N	Y	N	N
Vasanth et al. (2025) [123]	Optimize EV fleet delivery routing with AI	SA + heuristic path planning	AI	Y	N	Y	N	N
Singh et al. (2018) [55]	Blockchain + AI for intelligent vehicle communication	Local dynamic blockchain + encryption	Blockchain, AI	Y	Y	Y	N	N
Dorokhova et al. (2021) [124]	Blockchain-based EV charging management	Smart contracts on Ethereum	Blockchain	N	Y	Y	Y	N
AlSaif et al. (2021) [125]	Requirements for blockchain-based EV energy trading	Review analysis of blockchain potential	Blockchain	N	Y	Y	Y	N
Garg et al. (2019) [126]	Hierarchical EV charging authentication for V2G	ECC + blockchain hierarchical authentication	Blockchain	N	Y	Y	Y	N

(Continued)

Table 8 (continued)

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Martyushev et al. (2025) [127]	EV battery reliability modeling	Mathematical modeling	– (no tech keywords specified)	N	N	Y	N	N
Indushree et al. (2023) [128]	IoV cybersecurity & forensics using AI & blockchain	IDS + blockchain auth + DL models for forensics	Blockchain, AI	Y	Y	Y	N	Y

Note: 1: AI involved, 2: Blockchain involved, 3: Supply chain involved, 4: Traceability involved, 5: Forensic involved.

Besides, regulatory initiatives such as the EU's upcoming "battery passport" framework can leverage blockchain as a digital ledger platform to meet policy requirements and strengthen consumer trust.

4.4.1 AI and Blockchain for EV Component Traceability

In applying AI and blockchain to component traceability and data security in EV supply chains, Ref. [112] classified suppliers into three categories: chassis, drivetrain, and battery. The study initially deployed ANN, LSTM, and RNN algorithms to detect potentially malicious behavior among suppliers. Once identified, smart contracts were used to record component-related data on a blockchain. The immutability of the blockchain prevents any unauthorized alterations to component records, thus improving the transparency and traceability of the supply chain.

In response to traceability for lithium-ion battery raw materials, Ref. [113] proposed a theoretical framework based on a blockchain ecosystem to support future implementation and scholarly research on battery component traceability and recycling. Addressing risks such as child labor and environmental pollution in small-scale and artisanal mining regions, Ref. [114] demonstrated a blockchain-enabled system that tracks every stage of cobalt extraction by recording data such as mining locations, mining identities, working conditions, and ore sale and transport records. Data from mines, smelters, and markets are immutably logged on the blockchain ledger, enhancing both transparency and traceability. Synchronously, AI are proposed to analyze mining operations and identify potential legal or ethical violations. In a related application, Ref. [115] implemented a combination of blockchain and QR code technologies in EV the production of EVs. Batteries are laser-engraved with unique QR codes linked to a Traceability System that records raw materials and production data at each stage. The system leverages blockchain connectivity to document critical traceability points, such as material mixing, splitting, or transformation, in real time, thus preventing data loss or untraceable gaps. AI-driven modeling and data analysis are also used to predict product defects and enhance manufacturing quality.

In the context of circular economy and sustainable management, Ref. [116] examined the application of blockchain to monitor battery supply chains. The study demonstrated that blockchain enhances transparency and traceability throughout the life cycle of lithium-ion batteries—from resource extraction and manufacturing to recycling—thereby preventing environmental pollution and supporting sustainability objectives. Specifically, the blockchain records critical data at each stage, including mineral origin, processing parameters, transport logs, chemical composition, and pollution metrics. Meanwhile, Ref. [117] implemented a blockchain-based system to trace raw materials, production, and usage information throughout the full life cycle of lithium-ion EV batteries. This decentralized approach prevents unauthorized data modification and

implements a Digital Battery Passport on the chain, which logs the battery health status (State of Health), material composition, and recycling records—enhancing supply chain traceability and promoting circular economy principles. Furthermore, Ref. [118] integrated blockchain with QR-code by laser-etching a unique QR code onto each battery during manufacturing. Suppliers register information—such as the origins of hazardous materials (e.g., lead, tin, sulfuric acid)—on the blockchain ledger. Each logistics transfer is digitally signed and recorded, allowing verification by third-party auditors and strengthening regulatory oversight. In addition to this, AI-driven analytics can be employed to evaluate recycling processes and improve circular economy management.

4.4.2 AI and Blockchain Apply to SCM of EVs

In [119], the authors proposed a Life Cycle Tracking model for vehicle lifecycle management that integrates blockchain and ML. The model consists of three parts: user registration and authentication, blockchain-based data encryption, and verification of smart contracts driven by fuzzy logic Lukasiewicz driven smart contract verification. This framework enables multiple stakeholders across different stages of the supply chain to validate data, effectively supporting intelligent vehicle management and fraud detection in cloud-based environments. Coincidentally, Ref. [120] explored how AI combined with blockchain-based smart contracts can optimize operational efficiency and sustainability in the autonomous vehicle supply chain. The study introduced an innovative Margin Indicator designed to enhance the predictive accuracy of standard ML algorithms while using blockchain to control costs and manage energy consumption. Preliminary validation demonstrated that this system can reduce energy waste by approximately 12.5%.

To address disruption risks, Ref. [121] proposed the Schematic-based Hierarchical Induction for the EV supply chain Disruption system, which integrates large language models and graph convolutional networks. By employing schema learning and disruption analysis, the system predicts potential disruptions in EV battery supply chains, thereby improving the precision of risk assessment. Coincidentally, Ref. [122] examined the impact of AI on management of the automotive industry supply chain management using a mixed-methods approach that combined quantitative and qualitative analyzes. The study evaluated applications of ML, IoTs, and robotics, and emphasizes the role of AI in improving supply chain resilience and boosting manufacturing productivity.

4.4.3 AI and Blockchain Apply to Logistic of EVs

To effectively manage delivery fleets composed of multiple EVs and avoid inefficiencies such as excessive waiting and charging station congestion at charging stations, Ref. [123] proposed an AI-based Simulated Annealing algorithm to approximate optimal routing solutions. In conjunction with this, the authors also designed a set of local search heuristic algorithms, which significantly reduce the computation time while maintaining routing deviations within 25%. This combined strategy addresses vehicle heterogeneity—such as differences in battery levels and payload capacities—and optimizes travel time for urban delivery and return routes.

To address trust, security, and data integrity concerns in intelligent vehicle communications, Ref. [55] introduced a decentralized communication framework that integrates AI and blockchain. The framework employs a dual-layer architecture consisting of a Local Dynamic Blockchain and a main blockchain, and introduces encrypted identity tokens known as Intelligent Vehicle Trust Points. These mechanisms ensure secure and trusted interactions between vehicles without exposing personal information.

4.4.4 AI and Blockchain Apply to EV Energy Management

Ref. [111] systematically examined blockchain applications in the EV charging domain, highlighting the potential of the technology to support decentralized peer-to-peer energy trading platforms. This enables EV users to directly exchange energy, thus enhancing the utilization of renewable sources. In addition, blockchain facilitates the secure recording and verification of charging events, promoting transparency and mitigating fraud.

Extending this concept, Ref. [124] proposed an EV charging management framework built on Ethereum and Solidity smart contracts. This architecture enables the recording and settlement of trustless energy transactions between nodes, improving both efficiency and security of charging and billing, with the added benefit of reducing charging costs. The framework was successfully validated through a field demonstration in Switzerland.

Given that many current EV energy trading solutions rely on centralized architectures—lacking immutability, fault tolerance, and traceability and thus vulnerable to single-point failures and tampering, Ref. [125] analyzed blockchain's advantages in delivering transparent, immutable, decentralized, auditable, and confidential energy trading infrastructure for EVs.

Further advancing the field, Ref. [126] introduced a hierarchical, blockchain-based mutual authentication mechanism using elliptic curve cryptography for anonymized and secure charging station communications EV. The system leverages the blockchain ledger for decentralized verification of energy transactions, enhancing both security and efficiency in EV grid interactions. Lastly, Ref. [127] developed a smart battery management model to analyze the dynamic charge–discharge behavior of electric trucks under various urban and suburban driving conditions.

4.4.5 AI and Blockchain Apply to Forensic of IoV

The Internet of Vehicles (abbreviated as IoV) enables intelligent transportation by interconnecting vehicles, sensors, and users. However, it also introduces substantial cybersecurity risks, including spoofing attacks, privacy breaches, and authentication vulnerabilities. To address these threats, Ref. [128] proposed a comprehensive security and forensic framework for IoV that integrates an AI-driven intrusion detection system, blockchain-based authentication mechanisms and DL models. This multi-layered approach enhances real-time threat detection, ensures secure identity verification, and supports forensic investigation capabilities within vehicular networks.

4.5 AI and Blockchain Apply to UAVs

Although blockchain and AI technologies have been widely adopted in sectors such as agriculture, food, pharmaceuticals, and EVs for the traceability of components and raw materials, concerns persist regarding the accuracy of the data being recorded. The World Economic Forum, in its Blockchain Toolkit [129], explicitly states: “If the original data is inaccurate, storing it on a blockchain does not make it correct.” In parallel, the MIT Center for Transportation & Logistics, in its Supply Chain Management Roundtable Report [130], emphasizes the challenge of verifying the integrity of data entered into blockchain systems. The ongoing issue of origin mislabeling stems from the lax enforcement of country-of-origin labeling regulations by exporting countries, thereby diminishing the reliability of such information as forensic evidence.

In this regard, Refs. [52,53] propose a concept, methodology, and empirical validation for using another relationship to verify data independence—representing a promising direction for further exploration. From this perspective, verifiable independent data may include records of transportation time and distance, which can be marked by timestamps of arrival and departure at ports. These data points can serve as effective

forensic trails for legal applications. The required technologies involve IoT devices embedded in components to collect geotagged port information and timestamps, blockchain-based storage of these markers, port-side infrastructure to transmit geographic and temporal data, wireless communication between devices, and blockchain-based linkage of all port markers and timestamps for each product component (see Fig. 10 below). Relevant technologies can be referenced from existing IoT-based tracking systems [131], with substantial advancements already demonstrated in the UAV domain [132].

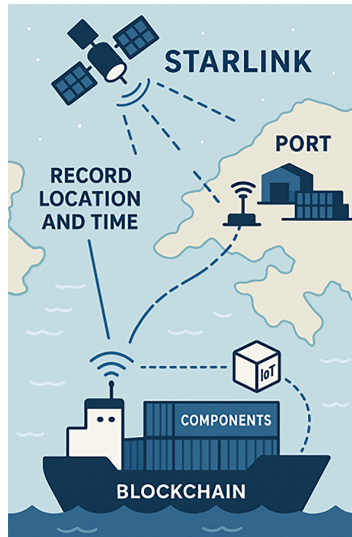


Figure 10: Recording geolocation and timestamps via IoT devices during vessel arrivals and departures at ports, serving as traceability data for subsequent origin analysis

4.5.1 UAV-Based Traceability of Origin

With regard to the traceability of UAV components, Ref. [133] proposes a blockchain-based solution utilizing non-fungible composable tokens to manage, certify and trace the origin, usage history, and ownership of UAV components. This approach aims to improve transparency within the supply chain and ensure the authenticity of individual parts (see Table 9 below). The study also incorporates digital twin to accurately reflect the status and evolution of physical assets. Ref. [134] explores the integration of blockchain and 6G communication systems into UAV applications. It highlights the critical role of blockchain in security verification and data integrity. Real-world logistics cases are presented to demonstrate the feasibility of using blockchain to record logistics journey data, thus supporting origin traceability.

Table 9: A relative comparison of approaches used to apply AI and blockchain in supply chain traceability and forensic contexts in UAV industry

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Hawashin et al. (2024) [133]	Ensure traceability and certification of UAV parts	Blockchain + NFT + Digital Twin	Blockchain, NFT, DT	N	Y	Y	Y	N
Aggarwal et al. (2021) [134]	Enhance UAV comms & logistics traceability	Blockchain + 6G for secure comms	Blockchain	N	Y	Y	Y	N

(Continued)

Table 9 (continued)

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Alzahrani et al. (2020) [132]	Enable sensor-based origin tracking via UAV	IoT sensors + Blockchain	Blockchain, IoT	N	Y	Y	Y	N
Alkadi et al. (2022) [135]	Achieve interoperability across UAV networks	Blockchain cross-chain framework	Blockchain	N	Y	Y	Y	N
Kumar et al. (2021) [136]	Secure UAV peer communication & GPS data	Ethereum-based P2P Blockchain	Blockchain	N	Y	Y	Y	N
Hashemi et al. (2023) [137]	Fault-tolerant air traffic for UAVs	Autoencoder + P2P Blockchain	Blockchain, AI	Y	Y	Y	Y	N
Fernández-Caramés et al. (2019) [138]	Use UAV + RFID + BC for traceable inventory	UAV + RFID + Blockchain + AI	Blockchain, RFID, AI	Y	Y	Y	Y	N
Hafeez et al. (2022) [139]	Authenticate secure UAV data flow	Smart contracts on blockchain	Blockchain	N	Y	Y	Y	N
Islam et al. (2020) [140]	Secure UAV-IoT healthcare data	UAV + Blockchain + Sensors	Blockchain, IoT	N	Y	Y	Y	N
Collins et al. (2025) [141]	Survey privacy-preserving federated learning for decentralized AI applications	Literature review and architecture analysis	Federated learning, differential privacy, secure aggregation	Y	N	N	N	N
Feng et al. (2022) [142]	Privacy-preserving FL across UAVs	BE-DHFL with Blockchain	Blockchain, AI	Y	Y	N	N	Y
Ferrag et al. (2021) [143]	Secure FL-based IDS in IoT/UAVs	Federated Deep Learning + Blockchain	Blockchain, AI	Y	Y	N	N	Y
Zhu et al. (2022) [144]	Improve MEC in UAV-FL using BC	FL + Blockchain consensus	Blockchain, FL	Y	Y	N	N	Y
Gupta et al. (2021) [145]	Secure drone networking under 5G	AI + IPFS + Blockchain	Blockchain, AI	Y	Y	N	N	Y
Xiao et al. (2021) [146]	UAV swarm for secure crowd monitoring	UAV + Blockchain + AI + 5G	Blockchain, AI	Y	Y	N	N	Y

(Continued)

Table 9 (continued)

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
He et al. (2025) [147]	Optimize UAV data transmission	DRL + LSTM path planning	AI	Y	N	N	N	N

Note: 1: AI involved, 2: Blockchain involved, 3: Supply chain involved, 4: Traceability involved, 5: Forensic involved.

Similarly, Ref. [132] conducts a comprehensive review of combination of UAVs with sensor-based IoTs to collaboratively collect and transmit “origin traceability data” to improve logistics transparency. The key topics addressed include: real-time acquisition of raw environmental data, creation of timestamped historical records, and real-time GPS data logging on the blockchain. This study advocates leveraging blockchain’s immutability to establish bidirectional trust in wireless communications between ground control stations and freight-carrying platforms. This, in turn, enables the creation of an “undeniable logistic history” that can serve as verifiable data input for blockchain-based traceability systems. Furthermore, it proposes a solution that integrates IoT devices and wireless communication technologies to record the logistics journey of each component during transportation, thereby achieving part-level traceability of the origin. Furthermore, Ref. [135] reviews recent developments and persistent challenges in blockchain interoperability within UAV systems. It proposes a cross-chain collaboration mechanism designed for multifunctional UAV platforms. The framework aims to reduce cross-chain operational costs, enhance compatibility among heterogeneous blockchain networks, support origin traceability, and enable multi-regional tracking.

UAVs commonly rely on the Global Positioning System (abbreviated as GPS) for navigation and positioning. To address the need for autonomous communication in remote environments, Ref. [136] proposes a secure communication framework based on the Ethereum blockchain, designed to counter GPS spoofing and related threats. The system utilizes the decentralized blockchain ledger to verify GPS data, enhancing resistance to signal interference and ensuring data integrity. It is also applicable to IoT-based logistics systems, enabling reliable wireless recording and transmission of logistics trajectory data while effectively detecting and isolating anomalous signal sources. In addition, Ref. [137] presents a fault-tolerant approach to flight trajectory data by integrating autoencoders with a blockchain structure. This method maintains reliability even in the cases of incomplete GPS data. To further enhance performance, sharding technology is employed to reduce on-chain computational complexity while improving system stability and conflict mitigation. This solution is particularly suited for addressing the GPS data gaps encountered during the recording of logistics journeys using IoT devices.

With regard to using IoTs and wireless communication to record and transmit logistics trajectory data, Ref. [138] designs a modular system that integrates UAVs, RFID scanners and blockchain. This system captures logistics data and records them on-chain to ensure verifiability and high-precision localization and to enable effective tracking of logistics processes. When combined with AI-based data analytics, the approach improves supply chain transparency and efficiency and supports origin traceability. Meanwhile, Ref. [139] introduces BETA-UA, a lightweight framework that utilizes smart contracts to manage data flow and prevent counterfeiting and replay attacks. This solution provides strong security assurances for UAVs while maintaining minimal resource consumption, and is applicable to IoT-based logistics tracking and origin verification. However, Ref. [140] applies blockchain to establish secure communication between UAVs and wearable sensors. Once verified, the collected data are transmitted to the nearest server and recorded on

the blockchain. This method ensures secure bidirectional communication between the IoTs and the port or airport infrastructure.

4.5.2 Federated Learning and Blockchain Apply to UAVs

Federated Learning is a decentralized machine learning approach [141] that enables multiple devices or institutions to collaboratively train models without exposing raw data. Each participant trains a local model and uploads only model parameters or gradients to a central server for aggregation, thus preserving data privacy and improving security. This technique is particularly well-suited for scenarios involving sensitive information—such as in healthcare, finance, and smart device applications—by balancing model performance with data protection.

In response to these concerns, Ref. [142] introduces a blockchain-enhanced cross-domain federated learning framework aimed at improving the privacy and security of 5G-enabled UAVs. Traditional federated learning approaches that rely on centralized servers are vulnerable to single points of failure, which can jeopardize the entire system. To mitigate this, the proposed framework employs blockchain and smart contracts to manage identity authentication and model aggregation across UAVs from different domains, effectively replacing the centralized aggregation server. Experimental results demonstrate robust performance in terms of cross-domain verification efficiency and accuracy, offering a secure and decentralized alternative.

Likewise, Ref. [143] reviews the application of FL in IoTs with a particular focus on data privacy and cybersecurity. Through empirical evaluation, the study shows that integrating FL with blockchain significantly improves intrusion detection accuracy while protecting user data, thus enhancing the security posture of IoT and UAV networks.

Additionally, traditional FL architectures are inherently dependent on central servers. Ref. [144] proposes a decentralized solution using blockchain's consensus and immutability features to replace central authority. This approach enables UAVs to participate in FL without sharing raw data, thereby enhancing privacy preservation and model trustworthiness within mobile edge computing environments.

4.5.3 AI-Blockchain Integration for Cybersecurity in UAV Communications

UAV wireless communication systems often face significant cybersecurity vulnerabilities and are generally unsuitable for computationally intensive encryption methods. Conventional blockchain-based solutions, while offering data integrity, frequently encounter limitations such as high storage costs and limited bandwidth. To address these threats, Ref. [145] proposes a blockchain-based data storage framework leveraging the Inter Planetary File System, integrated with an AI-enabled UAV communication architecture. This approach enhances the cybersecurity of UAV communication while reducing storage overhead and improving transmission efficiency.

Building on similar objectives, Ref. [146] presents an AI- and blockchain-enhanced UAV swarm collaboration system, where blockchain is used to prevent data manipulation during transmission and storage. Sensor data collected via IoT modules is transmitted to the system, while 5G networks enable AI-powered edge computing and real-time data analytics. The entire decision-making process is managed by smart contracts, ensuring secure, efficient, and transparent coordination among UAVs.

In addition, Ref. [147] addresses the optimization of data transmission in UAVs by proposing a deep reinforcement learning algorithm that integrates discrete and continuous action spaces. The model incorporates a LSTM network to support real-time flight path planning. The simulation results indicate that the proposed method improves the efficiency of data collection by up to 10.76% compared to traditional heuristic approaches.

4.6 Robots

Robots are AI products. Contemporary research focuses primarily on their applications in production processes and supply chains to enhance operational efficiency. UAVs, EVs, and robots are three categories of AI-driven technologies that could potentially be used during geopolitical conflicts if their control systems are compromised. These gray-zone conflicts constitute a cost-efficient yet highly effective military strategy. Among these technologies, only robots are designed to serve as companions to civilians in peacetime, and therefore, when hijacked and repurposed for hostile use, they can cause the most extensive damage. Ref. [148] categorizes the architecture of humanoid robots into three components: the Brain, the Body, and the Integrator. The Body comprises several critical parts, including sensors, batteries, actuators, encoders, gears/reducers, motors, and bearings. Among these, sensors, actuators, and reducers are particularly vulnerable to malicious code implantation, posing serious security risks by enabling remote control by adversaries at critical moments. For example, the Spanish cybersecurity firm Tarlogic Security reported that ESP32 chips manufactured in China contain hidden undocumented instructions, which could function as backdoors capable of remotely controlling millions of IoT devices [7].

Despite the severity of such risks, there is a lack of systematic research addressing the transparency of component origins in robot manufacturing (see Table 10 below). This represents a promising and underexplored area of inquiry, especially in the context of escalating geopolitical tensions and strategic competition over critical technologies—such as the technological decoupling between the United States and China. The integration of blockchain, digital twin systems, and supply chain traceability technologies can offer both significant academic contributions and practical value in securing the future of the robotics industry.

Table 10: A relative comparison of approaches used to apply AI and blockchain in supply chain traceability and forensic contexts in the robot industry

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Howard (2023) [148]	Identify national security risk in humanoid robot part supply	Value chain analysis	Robotics, IoT	Y	N	Y	Y	Y
Keshvarparast et al. (2024) [149]	Review cobots in manufacturing/assembly	Literature review	AI, robotics	Y	N	Y	N	N
Patel et al. (2018) [150]	Robots in various sectors through IoT	IoT + robotics integration	Robotics, IoT	Y	N	Y	N	N
Bernardo et al. (2022) [151]	Use of robots in internal logistics	Systematic literature review	Robotics, logistics	Y	N	Y	N	N
Aditya et al. (2021) [33]	Blockchain survey in robotics	Literature survey	Blockchain, robotics	N	Y	Y	N	N
Fernandes et al. (2019) [152]	RobotChain for AI behavior traceability	Tezos blockchain + AI	Blockchain, AI	Y	Y	N	Y	N

(Continued)

Table 10 (continued)

Authors/Year	Objective	Approach	Technology used	1	2	3	4	5
Lopes et al. (2019a) [153]	Detect robot anomalies through blockchain	Anomaly detection + RobotChain	Blockchain, robotics	N	Y	N	Y	Y
Lopes et al. (2019b) [154]	Monitor cobots via blockchain & 3D vision	RobotChain + computer vision	Blockchain, vision	Y	Y	N	Y	N
Lopes et al. (2021) [155]	Optimize storage of robot blockchain logs	Time-segmented blockchain	Blockchain, robotics	N	Y	N	N	N
Castelló Ferrer et al. (2018) [156]	Secure data sharing in robot interaction	RoboChain + ML	Blockchain, ML	Y	Y	N	N	Y
Castelló Ferrer (2016) [157]	Enable consensus in swarm robotics	Blockchain + crypto rules	Blockchain, swarm	N	Y	N	N	N
Castelló Ferrer et al. (2019) [158]	Secret cooperation in swarms via Merkle tree	Blockchain + Merkle proof	Blockchain, swarm	N	Y	N	N	Y
Peña Queralta et al. (2020) [159]	Enable fair collaboration in heterogeneous swarms	PoW + smart contracts	Blockchain, robotics	Y	Y	N	N	N
Pacheco et al. (2020) [160]	Prevent malicious behavior in robot swarm	Blockchain-controlled <i>ad-hoc</i> network	Blockchain, swarm	N	Y	N	N	Y

Note: 1: AI involved, 2: Blockchain involved, 3: Supply chain involved, 4: Traceability involved, 5: Forensic involved.

4.6.1 Robots Adopted in Manufacturing and Supply Chain

The advent of Industry 4.0 has introduced collaborative robot technologies (abbreviated as Cobot), positioning human–robot interaction as a key driver of industrial transformation. This development has significantly improved the flexibility and efficiency of both the assembly and disassembly processes. In response to these advances, Ref. [149] systematically reviewed the literature on the use of robots in the collaboration of the production line. The review covers several aspects, including improving Cobot performance through improvements in sensors, arm structure, and motion efficiency; increasing robot autonomy and adaptability via advanced algorithms and control logic; and enhancing the efficiency and safety of human–robot collaboration. It also emphasizes the need for future studies to investigate the performance implications of different collaborative scenarios. Extending this concept, robots have been applied in a wide range of domains, including healthcare, manufacturing, engineering, goods transportation, defense, and smart cities. In this context, Ref. [150] examined the operational models of collaboration between robotics and IoT on multiple platforms.

Through IoT integration, robots have acquired advanced capabilities in automation, mobility, perception, and actuation, allowing them to coordinate with other systems and deliver innovative solutions to modern industries. However, this convergence also introduces a series of challenges, such as standardization, data security, privacy protection, hardware configuration, and computational efficiency. To address these emerging complexities, Ref. [151] conducted a systematic review of the literature on the application of robotics in internal logistics. The study identifies several key insights: (1) semantic knowledge systems enable robots to comprehend the relationships among objects and tasks in their environment, which facilitates reasoning and human–robot knowledge sharing; (2) automated guided vehicles and autonomous mobile robots are currently the most prevalent platforms for mobile operations in internal logistics; and (3) Cobots are increasingly being deployed in logistics scenarios, where they can share workspaces and perform out collaborative tasks with human operators. The study recommends that future research should focus on robotic knowledge modeling, human–robot interface development, and the integration of advanced perception technologies.

4.6.2 Blockchain Applications in Robots

Robots are inherently AI products, and therefore, this subsection focuses specifically on the application of blockchain in robotics. Ref. [33] highlights that due to the limited computational resources of robots, sensory data often needs to be uploaded to cloud servers for processing. Although this centralized architecture enables efficient data sharing among multiple robots, it also presents significant challenges such as resource bottlenecks, single points of failure, and privacy and security concerns. Blockchain offers a decentralized alternative that improves data integrity and enables robotic systems to maintain operational stability even in the presence of partial node failures. In this context, the study reviewed the current state of blockchain applications in robotics and proposed eight future research directions to facilitate the integration and co-evolution of blockchain and robotic technologies.

Regarding RobotChain, Ref. [152] utilized the Tezos blockchain as the underlying protocol and smart contract execution platform, integrating it with AI modules to develop RobotChain—a system designed to record and monitor robotic behavior while supporting autonomous decision-making. The system leverages the immutability of blockchain to ensure the integrity and traceability of robotic activity logs. In a related application, Ref. [153] proposed using the RobotChain architecture to securely record robot events, ensuring that once data is written to the chain, it becomes tamper-proof. In addition, the system incorporates an anomaly detection module that uses on-chain data to identify abnormal behaviors in Cobots and assess their production efficiency. Based upon this concept, Ref. [154] developed a system that integrates blockchain, robotics, and computer vision, enabling Cobots to detect human intrusions into the workspace and autonomously adjust their behavior. The system employs a Tezos-based RobotChain to log all events and image summaries (e.g., hashed representations), thereby ensuring data immutability and traceability while reducing dependence on centralized monitoring. Through the use of smart contracts, the system autonomously records robotic events and executes control logic—such as slowing down or halting robot operations—without the need for human intervention. This mechanism contributes to improved safety in collaborative human–robot environments. Also, blockchain systems continuously accumulate large volumes of data. Although these historical data may be useful for human reference, robots typically require only recent information to operate effectively. Given the limited storage capacity of robotic nodes, it is essential to manage blockchain data in real time. Therefore, Ref. [155] proposed a time-segmented storage architecture for RobotChain, specifically designed to reduce the storage burden on robot systems while preserving access to relevant and up-to-date data for operational decision-making.

Robots hold significant potential in mobile health, where access to sensitive personal data enables improved interactive learning and more effective clinical interventions. However, the absence of a secure and privacy-preserving data-sharing architecture limits the ability of multiple robots to exchange knowledge and collaborate efficiently. In response, Ref. [156] proposed a decentralized framework that integrates RoboChain blockchain technology, open data, and machine learning. This framework enables multiple robots across different hospitals to engage in collaborative learning and model sharing without disclosing patient information, thus safeguarding data privacy while enhancing system intelligence.

4.6.3 Blockchain Applications in Swarm Robotics

Swarm robotics refers to systems composed of large numbers of autonomous robots that coordinate through simple local rules to achieve distributed collaboration. These robots collectively exhibit swarm intelligence—emergent behavior similar to that observed in ant colonies or bee swarms—enabling them to perform tasks such as exploration, construction, transportation, and environmental monitoring. However, characteristics such as decentralized control and collective decision-making pose significant challenges for real-world deployment. Addressing this, Ref. [157] proposed combining blockchain with cryptographic algorithms to allow decentralized robots to reach consensus without relying on centralized control, thus establishing a shared and trustworthy decision-making mechanism.

In addition, Ref. [158] applied Merkle trees to ensure secure and confidential collaboration among robot swarm. A Merkle tree, also known as a hash tree, is a binary tree structure in which each leaf node contains the hash of a data block. This structure is widely used in blockchain, cryptocurrencies, and distributed systems to ensure data integrity and efficient verification. In [158], swarm robot tasks are encapsulated within a verified Merkle tree structure, allowing the separation of task validation from task content, thus preserving data confidentiality. Within this system, each robot is required to exchange encrypted proofs to verify the legitimacy of its actions before participating in collaborative operations. A simulated object retrieval task was conducted to demonstrate that this approach enables effective swarm collaboration without disclosing the full details of the task.

Heterogeneous swarms of robots refer to collaborative multi-robot systems composed of units that differ in type, functionality, capabilities, or physical configuration. These robots may include various combinations of sensors, actuators, computational resources, energy sources, mobility mechanisms, or task-specific modules. Through task allocation and coordinated behavior, such systems are capable of executing complex missions that would be difficult for homogeneous swarms to achieve. To address these challenges, Ref. [159] proposed a consensus mechanism based on the proof-of-work algorithm to dynamically estimate the computational resources available in real-time for each robot. Environmental sensing data from multiple robots is integrated via smart contracts, enabling quality-based data ranking and trust assessment. This framework supports fair information exchange without disclosing hardware-level details and further ensures data reliability through cross-validation using sampled blockchain transaction data.

In a related study, Ref. [160] implemented a decentralized mobile *ad-hoc* network using the Ethereum blockchain to support a swarm system composed of Pi-Puck robots. The proposed framework is designed to detect and isolate Byzantine robots—those exhibiting abnormal, untrustworthy, or malicious behavior—in order to enhance the robustness and security of decentralized collaboration.

4.7 Practical Applications of AI and Blockchain

To strengthen the practical relevance of our study and address the reviewer's concern regarding real-world validation, we have expanded this section to highlight representative cases where AI and blockchain

solutions have been implemented or tested beyond simulation environments. These examples span across the pharmaceutical supply chain, electric vehicle (EV) battery lifecycle management, and UAV authentication in defense logistics, thereby demonstrating the applicability of the proposed concepts in diverse and safety-critical domains.

Blockchain-based distributed ledger technologies have been regarded as an ideal infrastructure for pharmaceutical supply chains; however, existing technologies remain insufficient to fully address practical challenges. To this end, PHTrack, a framework proposed in [161] and built upon Hyperledger Sawtooth, aims to enhance drug traceability and anti-counterfeiting. Notably, PHTrack emphasizes minimizing resource consumption while incorporating quantum-secure off-chain peer-to-peer communication among nodes. Ref. [161] experimentally demonstrated its effectiveness in providing real-time drug provenance verification and ensuring comprehensive tracking across the supply chain.

In addition, the reuse of end-of-life EV batteries can substantially reduce both environmental impacts and economic costs; however, it is constrained by the absence of reliable performance data, thereby underscoring the need for a standardized battery passport to address information asymmetry. Ref. [162] developed an experimental procedure to collect the critical data required to complete a battery passport, thereby enabling the assessment of end-of-life EV battery repurposing for applications such as mobile charging stations and forklift trucks. Experimental results further indicate that, at 25°C, repurposed batteries may extend their operational lifetime by up to 11 years, highlighting their potential to deliver added value and new applications within the framework of a circular economy.

From military defense perspective, existing UAVs encounter significant bottlenecks in achieving real-time identity verification, while blockchain-based solutions suffer from high latency and limited scalability. To overcome these challenges, Ref. [163] proposed the iBANDA framework, designed to counter identity spoofing and airspace security threats in urban UAV operations. Notably, experimental results show that iBANDA achieves a mean average precision of 99.5%, a recall of 100%, and an F1-score of 99.8%, with an inference time of only 0.021 s. Adversarial testing further demonstrates its resilience against Sybil attacks and GPS spoofing, maintaining a false acceptance rate below 2.5% and operational continuity above 96%, underscoring its effectiveness as a secure authentication mechanism for UAV navigation.

Taken together, these three representative cases illustrate how AI and blockchain have moved beyond simulation-based studies to tangible real-world applications in pharmaceuticals, energy, and defense logistics. They not only demonstrate the feasibility of the proposed approaches but also underscore their transformative potential in enhancing transparency, trust, and security across critical supply chains.

5 Open Issues, Challenges, and Future Directions

With the rapid advancement of AI and blockchain in supply chain transparency, traceability, and authentication applications, an increasing number of studies have produced concrete results. However, several challenges and limitations persist in real-world deployment and interdisciplinary integration. This study identifies key open issues and outlines potential directions for future research as follows:

(a) Complexity of Technological Integration and Interoperability Challenges

Currently, the integration of AI and blockchain remains largely confined to laboratory prototypes. When applied to complex, multi-tiered, and cross-border supply chain systems, operational challenges often arise, including architectural heterogeneity, data format incompatibilities, and limitations in computational resources. For example, blockchain's data storage and transmission efficiency may not meet real-time monitoring demands, while AI models require substantial computing power and high-quality training data—placing considerable demands on hardware infrastructure. Future research should prioritize modular

system architecture, standardized API interfaces, and the development of lightweight AI models (e.g., edge AI) to improve integration efficiency and scalability.

(b) Immaturity of Data Privacy and Access Control Mechanisms

While blockchain provides the advantages of immutability and transparent record-keeping, not all information within multi-stakeholder supply chains is suitable for public exposure. In sectors such as ICs, pharmaceuticals, military drones, and robotics, data often involves sensitive content or intellectual property that requires strict access control and advanced encryption mechanisms. Existing studies rarely address how to balance the transparency of blockchain with the need for AI-driven data sharing. Future research should explore the application of cryptographic techniques—such as zero-knowledge proofs, secure multi-party computation, and homomorphic encryption—to enable privacy-preserving solutions for supply chain management.

(c) Regulatory Integration and Legal Validity in Forensic Applications

This study highlights the potential of AI and blockchain to serve as legal forensic tools to record and preserve supply chain data, particularly in combating origin fraud, counterfeit components, and falsified pharmaceuticals. However, the recognition, admissibility, and procedural treatment of digital evidence vary significantly between jurisdictions. For example, can smart contract records on a blockchain carry the same legal weight as traditional documents? Can AI-generated anomaly reports be admissible as evidence in criminal proceedings? These questions remain largely unresolved, highlighting the early-stage alignment between legal frameworks and emerging technological infrastructures. Future research should promote interdisciplinary collaboration between legal scholars and technologists to explore design principles for verifiable AI and blockchain-based custody chains in the management of digital evidence.

(d) Model Bias and Data Quality Issues

AI relies heavily on the completeness and representativeness of the training data for accurate prediction and classification. However, supply chain data are often unstructured, heterogeneous in source and inconsistent in timeliness—factors that easily introduce model bias. In high-sensitivity industries such as UAV or IC manufacturing, national security concerns and commercial confidentiality may further restrict access to sufficient or well-annotated datasets, thereby reducing model performance and trustworthiness. Future research should focus on data preprocessing techniques, such as data cleaning, automated labeling, and transfer learning to improve model robustness under real-world data constraints.

(e) Challenges in Cross-Border and Cross-Industry Collaboration

The application of AI and blockchain in globalized supply chain traceability requires addressing cross-border data flows, regulatory discrepancies between jurisdictions, and cultural differences. For example, the European Union emphasizes personal data protection, while the United States prioritizes national security. The ability to flexibly adapt to varying legal requirements across national boundaries is critical for successful real-world implementation. To facilitate this, international organizations such as ISO, OECD, and WTO should take the lead in establishing a Trusted Supply Chain Framework. At the same time, academic and research communities are encouraged to contribute empirical case studies and propose standardized implementation guidelines.

(f) Future Research Recommendations

In response to the challenges mentioned above, this study proposes the following five key directions for future research:

- (1) Develop modular and scalable system architectures that can support various industrial scenarios, including ICs, pharmaceuticals, EVs, UAVs, and robotics.

- (2) Ensure the traceability and transparency of AI decision-making processes, thereby enhancing their admissibility and credibility in legal and forensic contexts.
- (3) Design blockchain-based proof-of-origin ledgers with embedded forensic capabilities to combat origin laundering and product mislabeling.
- (4) Develop smart contract modules capable that are sensitive to jurisdictions and capable of adjusting to varying legal compliance requirements and supporting cross-border trade.
- (5) Integrate AI ethics and digital governance principles to establish a collaborative global framework and governance platform for supply chain transparency.

5.1 Interoperability and Integration Challenges across Sectors

All five sectors reviewed in this study—ICs, pharmaceuticals, EVs, UAVs, and robotics—share a common vulnerability: origin opacity that can result in national security threats and counterfeit risks. Examples include falsified drugs in the pharmaceutical sector or adversarial components embedded in ICs, EVs, UAVs, and robotics. This theme of supply chain transparency and provenance forensics has been emphasized throughout the manuscript. Nevertheless, when considering interoperability and integration across industries, several challenges arise that merit further discussion.

First, there are substantial differences in data formats, standards, and regulatory requirements across industries. Pharmaceutical traceability is centered on batch numbers and distribution nodes under frameworks such as the DSCSA and EU FMD, whereas EV battery supply chains increasingly rely on “battery passports” with performance indicators. UAV traceability emphasizes component certification and flight control data. Integrating such heterogeneous data into a unified blockchain or cross-chain system presents significant technical and organizational challenges.

Second, different industries may adopt distinct blockchain frameworks. For instance, pharmaceutical supply chains often rely on Hyperledger Fabric, while EV battery passports are being explored through decentralized European platforms. Without robust cross-chain protocols, it is difficult to achieve meaningful data sharing. Moreover, such integration is typically driven only when practical demand for inter-industry collaboration arises. Third, each sector falls under the jurisdiction of different regulatory authorities (e.g., FDA, NHTSA, EASA, ISO, IEC), with varying legal requirements for provenance evidence. Meeting multiple and sometimes conflicting regulatory standards simultaneously poses an additional layer of complexity for interoperability.

In summary, while the five industries share a common concern regarding supply chain transparency and origin forensics, the pursuit of interoperability and integration faces practical constraints rooted in heterogeneous data structures, divergent technological frameworks, and fragmented regulatory environments. These limitations underscore that future cross-sector traceability efforts will require both technological advances and policy harmonization to achieve meaningful integration.

5.2 Sector-Prioritized Future Research Directions

Building upon the cross-industry synthesis presented in [Section 4](#), future research directions should be prioritized at the sectoral level to address domain-specific gaps and policy imperatives:

- (a) Integrated Circuits (ICs): Future studies should focus on lightweight and verifiable forensic mechanisms that enhance chip authentication at scale, including tamper-evident cryptographic proofs and zero-trust architectures for outsourced fabrication. The integration of explainable AI (XAI) can help interpret anomaly detection results in hardware Trojan detection, improving both transparency and regulatory acceptance.

- (b) **Pharmaceuticals:** Research should emphasize explainable AI models integrated with blockchain to increase trust in counterfeit detection and regulatory compliance. For example, interpretable ML algorithms can support pharmaceutical traceability systems by providing regulators with auditable rationales for high-risk drug classifications, thereby bridging the gap between technical advances and legal adoption.
- (c) **EVs:** In addition to modular digital battery passports and lifecycle traceability systems, EV supply chains should adopt federated learning-based frameworks to improve collaborative intelligence across geographically distributed actors while preserving data privacy. Federated learning, when combined with blockchain for decentralized trust, can strengthen predictive maintenance, demand forecasting, and battery recycling analytics. Recent work has categorized blockchain-based federated learning into multiple application domains and demonstrated its potential to balance privacy, security, and efficiency in distributed environments [164].
- (d) **UAVs:** Future efforts should prioritize cross-chain interoperability and federated learning approaches to improve collaborative decision-making across heterogeneous UAV fleets. Blockchain-enabled federated learning can address the dual challenge of safeguarding sensitive data while enhancing swarm-level situational awareness, particularly in military and logistics applications.
- (e) **Robotics:** Research should extend toward supply chain provenance of robotic components, where blockchain-enabled RobotChain systems may ensure component authenticity and operational transparency. In addition, the convergence of swarm robotics with blockchain consensus mechanisms presents opportunities to achieve decentralized, resilient, and tamper-resistant coordination in critical infrastructure contexts.

Taken together, these sector-specific directions highlight that while AI–blockchain integration is a common enabler, the research priorities differ significantly by domain. Aligning future studies with these differentiated needs can maximize both academic contributions and policy relevance.

6 Conclusions

This study conducted a systematic review and analysis of the literature on applications of AI and blockchain in provenance tracking and forensic verification within the supply chains of sensitive industries, including ICs, pharmaceuticals, EVs, UAVs, and robotics. In light of increasing geopolitical tensions, escalating risks of supply chain disruption and the increasing prevalence of illicit activities such as counterfeiting and origin laundering, the establishment of reliable and forensically capable traceability systems has become an urgent priority for both policy makers and industry stakeholders. This research successfully achieved the two objectives outlined in [Section 1](#):

- (a) **To systematically integrate and categorize the current applications of AI and blockchain in supply chain traceability:** Based on a comprehensive review of 116 representative studies in high-sensitivity sectors—including ICs, pharmaceuticals, EVs, UAVs, and robotics—this study developed a classification framework based on application domains, technical architectures and functional objectives. It systematically presents how AI and blockchain technologies are integrated and applied in origin verification, legal forensics, data transparency, anti-counterfeiting, and decision-making optimization.
- (b) **To examine IC provenance and forensic technologies and assess their potential and challenges in detecting origin laundering:** This study synthesizes existing research on IC provenance and forensic mechanisms, exploring how AI and blockchain can be used to preserve chip manufacturing evidence and prevent counterfeiting and illicit circulation. A feasible framework is also proposed that integrates PUF, trusted platform modules, and smart contracts for legal forensics and origin verification.

The primary contribution of this study lies in its novel integration of AI, blockchain, and legal forensic technologies to conduct a cross-industry comparison and develop a technological roadmap for supply chains characterized by the relevance of national security and high-risk attributes. This research addresses a critical gap in the literature, where prior studies have often been fragmented and lack in-depth integration. By proposing a feasible system architecture and offering policy-relevant insights, the study provides both theoretical and practical value.

For future research, several directions are recommended:

- (a) The design of lightweight and deployable system architectures suitable for real-world implementation;
- (b) Examination of the cross-jurisdictional legal applicability of integrating AI-based decision-making with blockchain-based chains of evidence;
- (c) Development of multi-party verification platforms and cross-industry smart contract templates;
- (d) Establishment of open datasets and simulation environments to support empirical research and standard-setting in both academia and industry.

It is hoped that this study will serve as a foundation for advancing transparent governance, technological innovation, and policy formulation in high-sensitivity supply chains and contribute to the development of a reliable and accountable global supply chain infrastructure.

In addition, this study explicitly links sector-specific challenges with actionable Policy Recommendations, addressing gaps identified in prior research. This study highlights that while AI and blockchain technologies offer promising solutions for enhancing provenance traceability and forensic verification, sector-specific barriers necessitate differentiated policy responses (see [Fig. 11](#) below).

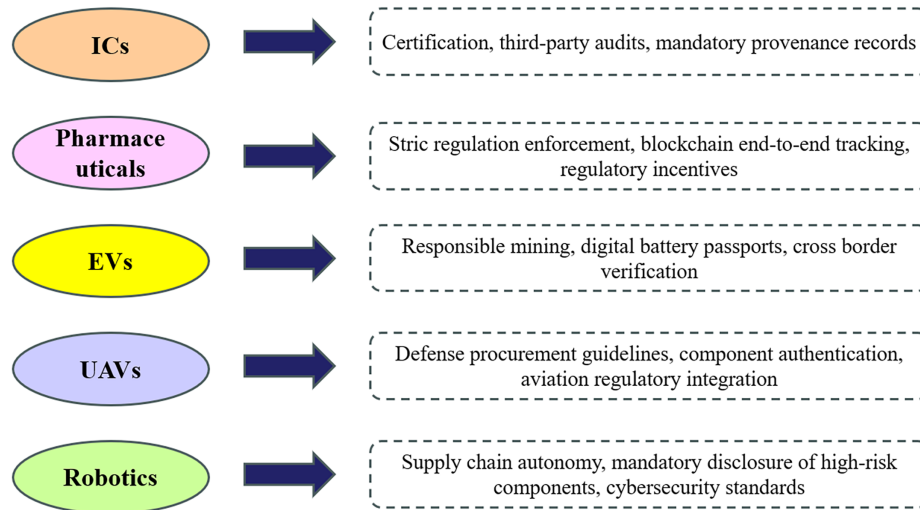


Figure 11: Sector-linked policy map

- (a) For IC supply chains, the primary risks involve hardware Trojans and counterfeits; thus, governments and industry bodies should establish international certification mechanisms, third-party audits, and mandatory provenance records to ensure chip authenticity.
- (b) In the pharmaceutical sector, widespread counterfeit drugs and cold-chain vulnerabilities underscore the need for rigorous implementation of regulatory frameworks such as the U.S. Drug Supply Chain Security Act and the EU Falsified Medicines Directive, coupled with incentives for blockchain-enabled end-to-end tracking systems.

- (c) For EV supply chains, human-rights controversies and environmental pollution in raw material sourcing and the traceability requirements of battery passports demand policy instruments that enforce responsible mining, standardized digital passports, and cross-border verification mechanisms.
- (d) UAV supply chains face acute challenges in airspace security and component verification, suggesting the necessity of defense procurement guidelines, component-level authentication standards, and integration with aviation regulatory frameworks (e.g., Federal Aviation Administration, European Union Aviation Safety Agency, and International Civil Aviation Organization).
- (e) For robotics, the absence of transparency in component sourcing poses both economic and security risks, calling for policies that promote supply chain autonomy, mandatory disclosure of high-risk components, and international cooperation on cybersecurity standards. By directly mapping these sectoral challenges to actionable policy measures, this study provides practical guidance for regulators and stakeholders aiming to enhance supply chain transparency, resilience, and security in strategically sensitive industries.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors' contributions are summarized below. Hsiao-Chun Han, Der-Chen Huang and Chin-Ling Chen made substantial contributions to the conception and design. Hsiao-Chun Han was involved in drafting the manuscript. Hsiao-Chun Han and Der-Chen Huang acquired data and analysis and conducted the interpretation of the data. The critically important intellectual contents of this manuscript were revised by Chin-Ling Chen. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data used in the study are IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library, Web of Science, and arXiv.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Statista Research Department. Revenue of the U.S. pharmaceuticals market from 2017 to 2034. [cited 2025 May 1]. Available from: <https://www.statista.com/statistics/1124374/us-pharmaceutical-market-size/>.
2. Grand View Research. Integrated circuits market size, share & trends analysis report, 2024–2034. [cited 2025 May 1]. Available from: <https://www.grandviewresearch.com/industry-analysis/integrated-circuits-market>.
3. BloombergNEF. Electric vehicle outlook 2024. [cited 2025 May 1]. Available from: <https://about.bnef.com/electric-vehicle-outlook/>.
4. Fortune Business Insights. Commercial drones market size, share, and COVID-19 impact analysis, 2024–2034. [cited 2025 May 1]. Available from: <https://www.fortunebusinessinsights.com/commercial-drone-market-102587>.
5. Markets and Markets. Industrial robotics market size & growth forecast, 2024–2034. [cited 2025 May 1]. Available from: <https://www.marketsandmarkets.com/Market-Reports/industrial-robotics-market-643.html>.
6. Heritage A. Skyrocketing pharmaceutical imports to the U.S. endanger national security [Internet]. Washington, DC, USA: Coalition for a Prosperous America; 2023 [cited 2025 Jun 8]. Available from: https://prosperousamerica.org/skyrocketing-pharmaceutical-imports-to-the-u-s-endanger-national-security/?utm_source=chatgpt.com.
7. Tarlogic Security. Tarlogic detects a hidden feature in the mass-market ESP32 chip that could infect millions of IoT devices; 2025 [Internet]. [cited 2025 May 28]. Available from: <https://www.tarlogic.com/news/hidden-feature-esp32-chip-infect-ot-devices/>.

8. O'Donnell J, Tanz LJ, Miller KD, Dinwiddie AT, Wolff J, Mital S, et al. Drug overdose deaths with evidence of counterfeit pill use—United States, July 2019–December 2021. *Morb Mortal Wkly Rep.* 2023;72(35):949–56. doi:10.15585/mmwr.mm7235a3.
9. Pathak R, Gaur V, Sankrityayan H, Gogtay J. Tackling counterfeit drugs: the challenges and possibilities. *Pharm Med.* 2023;37(4):281–90. doi:10.1007/s40290-023-00468-w.
10. Abbas K, Afaq M, Khan TA, Song WC. A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry. *Electronics.* 2020;9(5):852. doi:10.3390/electronics9050852.
11. Jamil F, Hang L, Kim K, Kim D. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. *Electronics.* 2019;8(5):505. doi:10.3390/electronics8050505.
12. Socal MP, Sharfstein JM. Drug shortages—a study in complexity. *JAMA Netw Open.* 2024;7(4):e244168. doi:10.1001/jamanetworkopen.2024.4168.
13. U.S. Food and Drug Administration. Drug supply chain security act (DSCSA). Silver Spring, MD, USA: FDA; 2013.
14. European Commission. Directive 2011/62/EU on falsified medicinal products. Brussels, Belgium: European Union; 2011.
15. World Health Organization. Substandard and falsified medical products. Geneva, Switzerland: WHO; 2017.
16. Tseng JH, Liao YC, Chong B, Liao SW. Governance on the drug supply chain via gcoin blockchain. *Int J Environ Res Public Health.* 2018;15(6):1055. doi:10.3390/ijerph15061055.
17. Coffin D, Downing D, Horowitz J, LaRocca G. The roadblocks of the COVID-19 pandemic in the U.S. automotive industry. Washington, DC, USA: U.S. International Trade Commission, Office of Industries; 2022. Report No.: ID-091.
18. Amnesty International. This is what we die for: human rights abuses in the Democratic Republic of the Congo power the global trade in cobalt. London, UK: Amnesty International; 2016.
19. Organization for Economic Co-operation and Development (OECD). OECD due diligence guidance for responsible supply chains of minerals from conflict-affected and high-risk areas. 3rd ed. Paris, France: OECD Publishing; 2016.
20. European Parliament and Council of the European Union. Regulation (EU) 2023/1542 concerning batteries and waste batteries. Brussels, Belgium: European Union; 2023.
21. U.S. Congress. Inflation reduction act of 2022, public law No.: 117-169. Washington, DC, USA: U.S. Government Publishing Office; 2022.
22. National Institute of Standards and Technology (NIST). Guide to industrial control systems (ICS) security (NIST SP 800-82 Rev. 2). Gaithersburg, MD, USA: NIST; 2015 [cited 2025 May 1]. Available from: <https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final>.
23. European Commission. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act). Brussels, Belgium: European Commission; 2021 [cited 2025 May 1]. Available from: [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.COM\(2021\) 206 final](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.COM(2021) 206 final).
24. European Union Agency for Cybersecurity (ENISA). Cybersecurity for robotics and autonomous systems. Athens, Greece: ENISA; 2020 [cited 2025 May 1]. Available from: <https://www.enisa.europa.eu/publications/cybersecurity-for-robots>.
25. Cabinet Office of Japan. Science, technology and innovation white paper 2020. Tokyo, Japan: Cabinet Office of Japan; 2020 [cited 2025 May 1]. Available from: https://data.e-gov.go.jp/data/dataset/mext_20221124_0008.
26. Ressi D, Romanello R, Piazza C, Rossi S. AI-enhanced blockchain technology: a review of advancements and opportunities. *J Netw Comput Appl.* 2024;225:103858. doi:10.1016/j.jnca.2024.103858.
27. Charles V, Emrouznejad A, Gherman T. A critical analysis of the integration of blockchain and artificial intelligence for supply chain. *Ann Oper Res.* 2023;327(1):7–47. doi:10.1007/s10479-023-05169-w.
28. Choi N, Kim H. Technological convergence of blockchain and artificial intelligence: a review and challenges. *Electronics.* 2025;14(1):84. doi:10.3390/electronics14010084.

29. Kayikci S, Khoshgoftaar TM. Blockchain meets machine learning: a survey. *J Big Data*. 2024;11(1):9. doi:10.1186/s40537-023-00852-y.
30. Abdelhamid M, Sliman L, Ben Djemaa R, Perboli G. A review on blockchain technology, current challenges, and AI-driven solutions. *ACM Comput Surv*. 2024;57(3):1–39. doi:10.1145/3700641.
31. Hafeez S, Khan AR, Al-Quraan MM, Mohjazi L, Zoha A, Ali Imran M, et al. Blockchain-assisted UAV communication systems: a comprehensive survey. *IEEE Open J Veh Technol*. 2023;4:558–80. doi:10.1109/OJVT.2023.3295208.
32. Singh AR, Kumar RS, Madhavi KR, Alsaif F, Bajaj M, Zaitsev I. Optimizing demand response and load balancing in smart EV charging networks using AI integrated blockchain framework. *Sci Rep*. 2024;14(1):31768. doi:10.1038/s41598-024-82257-2.
33. Srinivas Aditya USP, Singh R, Singh PK, Kalla A. A survey on blockchain in robotics: issues, opportunities, challenges and future directions. *J Netw Comput Appl*. 2021;196:103245. doi:10.1016/j.jnca.2021.103245.
34. Bhalerao P, Shinde J, Ghodke A, Balote S. Blockchain and AI in pharmaceutical supply chain. *Int J Sci Res Eng Trends*. 2024;10(3):158–63.
35. Kuznetsov O, Sernani P, Romeo L, Frontoni E, Mancini A. On the integration of artificial intelligence and blockchain technology: a perspective about security. *IEEE Access*. 2024;12:3881–97. doi:10.1109/ACCESS.2023.3349019.
36. Kuznetsov O, Sernani P, Romeo L, Frontoni E, Mancini A. A comprehensive review on artificial intelligence and blockchain technologies for electric vehicle charging ecosystems. In: *Comprehensive review of electric vehicle technology and its impacts: detailed investigation of charging infrastructure, power management, and control techniques*. Hershey, PA, USA: IGI Global; 2023. doi:10.4018/979-8-3693-2611-4.ch013.
37. Zuo Y, Guo J, Gao N, Zhu Y, Jin S, Li X. A survey of blockchain and artificial intelligence for 6G wireless communications. *IEEE Commun Surv Tutor*. 2023;25(4):2494–528. doi:10.1109/COMST.2023.3315374.
38. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. *SSRN Electron J*. 2008. doi:10.2139/ssrn.3440802.
39. Karaduman Ö, Gülhas G. Blockchain-enabled supply chain management: a review of security, traceability, and data integrity amid the evolving systemic demand. *Appl Sci*. 2025;15(9):5168. doi:10.3390/app15095168.
40. Jordan MI, Mitchell TM. Machine learning: trends, perspectives, and prospects. *Science*. 2015;349(6245):255–60. doi:10.1126/science.aaa8415.
41. Zhang Z, Song X, Liu L, Yin J, Wang Y, Lan D. Recent advances in blockchain and artificial intelligence integration: feasibility analysis, research issues, applications, challenges, and future work. *Secur Commun Netw*. 2021;2021(1):9991535. doi:10.1155/2021/9991535.
42. Rekha SS, Suraj K, Sudeendra Kumar K. A holistic blockchain based IC traceability technique. In: *2021 IEEE International Symposium on Smart Electronic Systems (iSES)*; 2021 Dec 18–22; Jaipur, India. doi:10.1109/iSES52644.2021.00078.
43. IEA. Global EV outlook 2025. Paris, France: International Energy Agency; 2025 [cited 2025 May 1]. Available from: <https://www.iea.org/reports/global-ev-outlook-2025>.
44. Shakhathreh H, Sawalmeh A, Al-Fuqaha A, Dou Z, Almaita E, Khalil I, et al. Unmanned aerial vehicles: a survey on civil applications and key research challenges. *arXiv:1805.00881*. 2018. doi:10.48550/arxiv.1805.00881.
45. Montini E, Daniele F, Agbomemewa L, Confalonieri M, Cutrona V, Bettoni A, et al. Collaborative robotics: a survey from literature and practitioners perspectives. *J Intell Rob Syst*. 2024;110(3):117. doi:10.1007/s10846-024-02141-z.
46. Reuters. Global robot investments top \$2.26 billion in Q1 2025, focus shifts to specialized applications. [cited 2025 Jun 25]. Available from: <https://www.reuters.com/world/china/nvidia-foxconn-talks-deploy-humanoid-robots-houston-ai-server-making-plant-2025-06-20/>.
47. Mehta P, Gupta R, Tanwar S. Blockchain envisioned UAV networks: challenges, solutions, and comparisons. *Comput Commun*. 2020;151:518–38. doi:10.1016/j.comcom.2020.01.023.
48. Sabogal De La Pava ML, Tucker EL. Effects of geopolitical strain on global pharmaceutical supply chain design and drug shortages. *Eur J Oper Res*. 2025;327(2):641–54. doi:10.1016/j.ejor.2025.05.002.
49. Bargujara N, Kalwar MA, Dermitzakis I, Nawaz A. The impact of the Russia-Ukraine war on the Russian supply chain. *J Emerg Sci Eng*. 2024;3(1):e33. doi:10.61435/jese.2025.e33.

50. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics Inform.* 2019;36:55–81. doi:10.1016/j.tele.2018.11.006.
51. Chen RY. A traceability chain algorithm for artificial neural networks using T-S fuzzy cognitive maps in blockchain. *Future Gener Comput Syst.* 2018;80:198–210. doi:10.1016/j.future.2017.09.077.
52. Han HC, Huang DC. Graph-theoretic detection of anomalies in supply chains: a PoR-based approach using Laplacian flow and sheaf theory. *Mathematics.* 2025;13(11):1795. doi:10.3390/math13111795.
53. Han HC, Huang DC. The blockchain neural network superior to deep learning for improving the trust of supply chain. *Comput Model Eng Sci.* 2025;143(3):3921–41. doi:10.32604/cmesci.2025.065627.
54. Tan Y, Gu L, Xu S, Li M. Supply chain inventory management from the perspective of “cloud supply chain”—a data driven approach. *Mathematics.* 2024;12(4):573. doi:10.3390/math12040573.
55. Singh M, Kim S. Branch based blockchain technology in intelligent vehicle. *Comput Netw.* 2018;145:219–31. doi:10.1016/j.comnet.2018.08.016.
56. Barron Y. Integrating replenishment policy and maintenance services in a stochastic inventory system with bilateral movements. *Mathematics.* 2023;11(4):864. doi:10.3390/math11040864.
57. Baghizadeh K, Ebadi N, Zimon D, Jum'a L. Using four metaheuristic algorithms to reduce supplier disruption risk in a mathematical inventory model for supplying spare parts. *Mathematics.* 2023;11(1):42. doi:10.3390/math11010042.
58. Harikrishnan T, Jeganathan K, Selvakumar S, Anbazhagan N, Cho W, Joshi GP, et al. Analysis of stochastic M/M/c/N inventory system with queue-dependent server activation, multi-threshold stages and optional retrieval facility. *Mathematics.* 2022;10(15):2682. doi:10.3390/math10152682.
59. European Commission. Regulation (EC) No. 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law. *Off J Eur Communities.* 2002;L31:1–24.
60. U.S. Food and Drug Administration. FDA food safety modernization act (FSMA). Public Law 111–353; 2011 [cited 2025 May 1]. Available from: <https://www.fda.gov/food/guidance-regulation-food-and-dietary-supplements/food-safety-modernization-act-fsma>.
61. Roy V, Tata SV, Parsad C. Consumer response to brand involved in food safety scandal: an exploratory study based on a recent scandal in India. *J Consum Behav.* 2018;17(1):25–33. doi:10.1002/cb.1666.
62. Khan PW, Byun YC, Park N. IoT-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning. *Sensors.* 2020;20(10):2990. doi:10.3390/s20102990.
63. Ugochukwu NA, Goyal SB, Rajawat AS, Islam SMN, He J, Aslam M. An innovative blockchain-based secured logistics management architecture: utilizing an RSA asymmetric encryption method. *Mathematics.* 2022;10(24):4670. doi:10.3390/math10244670.
64. Rodriguez-Aguilar R, Marmolejo-Saucedo JA, Köse U. Development of a digital twin driven by a deep learning model for fault diagnosis of electro-hydrostatic actuators. *Mathematics.* 2024;12(19):3124. doi:10.3390/math12193124.
65. Tian F. 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 (ICSSSM); 2016 Jun 24–26; Kunming, China. doi:10.1109/ICSSSM.2016.7538424.
66. Monteiro ES, da Rosa Righi R, Barbosa JLV, Alberti AM. APTM: a model for pervasive traceability of agrochemicals. *Appl Sci.* 2021;11(17):8149. doi:10.3390/app11178149.
67. Shahbazi Z, Byun YC. A procedure for tracing supply chains for perishable food based on blockchain, machine learning and fuzzy logic. *Electronics.* 2021;10(1):41. doi:10.3390/electronics10010041.
68. Sun Y, Song X, Jiang Y, Guo J. Strategy analysis of fresh agricultural enterprises in a competitive circumstance: the impact of blockchain and consumer traceability preferences. *Mathematics.* 2023;11(5):1090. doi:10.3390/math11051090.
69. Chen H, Chen Z, Lin F, Zhuang P. Effective management for blockchain-based agri-food supply chains using deep reinforcement learning. *IEEE Access.* 2021;9:36008–18. doi:10.1109/ACCESS.2021.3062410.
70. Tian X, Guan Y, Wang S. A decision-focused learning framework for vessel selection problem. *Mathematics.* 2023;11(16):3503. doi:10.3390/math11163503.

71. Bamakan SMH, Faregh N, ZareRavasan A. Di-ANFIS: an integrated blockchain-IoT-big data-enabled framework for evaluating service supply chain performance. *J Comput Des Eng.* 2021;8(2):676–90. doi:10.1093/jcde/qwab007.
72. Chidepatil A, Bindra P, Kulkarni D, Qazi M, Kshirsagar M, Sankaran K. From trash to cash: how blockchain and multi-sensor-driven artificial intelligence can transform circular economy of plastic waste? *Adm Sci.* 2020;10(2):23. doi:10.3390/admsci10020023.
73. Dey S, Saha S, Singh AK, McDonald-Maier K. SmartNoshWaste: using blockchain, machine learning, cloud computing and QR code to reduce food waste in decentralized web 3.0 enabled smart cities. *Smart Cities.* 2022;5(1):162–76. doi:10.3390/smartcities5010011.
74. Kamble SS, Gunasekaran A, Parekh H, Mani V, Belhadi A, Sharma R. Digital twin for sustainable manufacturing supply chains: current trends, future perspectives, and an implementation framework. *Technol Forecast Soc Change.* 2022;176:121448. doi:10.1016/j.techfore.2021.121448.
75. Wong S, Yeung JKW, Lau YY, So J. Technical sustainability of cloud-based blockchain integrated with machine learning for supply chain management. *Sustainability.* 2021;13(15):8270. doi:10.3390/su13158270.
76. Ivanov D, Dolgui A, Sokolov B. The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *Int J Prod Res.* 2019;57(3):829–46. doi:10.1080/00207543.2018.1488086.
77. Rodríguez-Espíndola O, Chowdhury S, Beltagui A, Albores P. The potential of emergent disruptive technologies for humanitarian supply chains: the integration of blockchain, artificial intelligence and 3D printing. *Int J Prod Res.* 2020;58(15):4610–30. doi:10.1080/00207543.2020.1761565.
78. Helinski RL, Cole EI, Robertson G, Woodbridge J, Pierson LG. Electronic forensic techniques for manufacturer attribution. In: 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST); 2016 May 3–5; McLean, VA, USA. p. 139–44. doi:10.1109/HST.2016.7495572.
79. Bloom G, Narahari B, Simha R. Fab forensics: increasing trust in IC fabrication. In: 2010 IEEE International Conference on Technologies for Homeland Security (HST); 2010 Nov 8–10; Waltham, MA, USA. p. 99–105. doi:10.1109/THS.2010.5655082.
80. Shandilya R, Sharma RK. Secure chip to chip communication based on zero trust architecture in sensor network. In: 2025 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS); 2025 Jan 18–19; Bhopal, India. doi:10.1109/SCEECS64059.2025.10941207.
81. Kulkarni A, Ahmad Hazari N, Niamat M. A blockchain technology approach for the security and trust of the IC supply chain. In: 2019 IEEE National Aerospace and Electronics Conference (NAECON); 2019 Jul 15–19; Dayton, OH, USA. p. 249–52. doi:10.1109/naecon46414.2019.9058027.
82. Dangi S, Ghanshala K, Sharma S. HOLMES: artificial intelligence enabled expert system for efficient acquisition and analysis using live memory forensics. In: 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET); 2024 Jun 7–8; Nagpur, India. doi:10.1109/ICICET59348.2024.10616275.
83. Kulkarni A, Ahmad Hazari N, Niamat M. Ring oscillator PUF and blockchain: a way of securing post fabrication FPGA supply chain. In: 2023 IEEE 66th International Midwest Symposium on Circuits and Systems (MWSCAS); 2023 Aug 6–9; Tempe, AZ, USA. doi:10.1109/MWSCAS57524.2023.10405953.
84. Kulkarni A, Ahmad Hazari N, Niamat MY. A zero trust-based framework employing blockchain technology and ring oscillator physical unclonable functions for security of field programmable gate array supply chain. *IEEE Access.* 2024;12:89322–38. doi:10.1109/ACCESS.2024.3418572.
85. Khan AA, Uddin M, Shaikh AA, Ali Laghari A, Rajput AE. MF-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture. *IEEE Access.* 2021;9:103637–50. doi:10.1109/ACCESS.2021.3099037.
86. Ab Rahman NH, Glisson WB, Yang Y, Choo KR. Forensic-by-design framework for cyber-physical cloud systems. *IEEE Cloud Comput.* 2016;3(1):50–9. doi:10.1109/MCC.2016.5.
87. Nelufule N, Singano T, Masemola K, Shadung D, Nkwe B, Mokoena J. An adaptive digital forensic framework for the evolving digital landscape in Industry 4.0 and 5.0. In: 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT); 2024 Jan 4–6; Bengaluru, India. doi:10.1109/IDCIoT59759.2024.10467482.

88. Dave M. Internet of Things security and forensics: concern and challenges for inspecting cyber attacks. In: 2022 Second International Conference on Next Generation Intelligent Systems (ICNGIS); 2022 Jul 29–31; Kottayam, India. doi:10.1109/ICNGIS54955.2022.10079829.
89. Sonawane A, Lakade N, Sarkar S, Dongre N. Securing digital evidence in forensic investigation using blockchain. In: 2024 4th Asian Conference on Innovation in Technology (ASIANCON); 2024 Aug 23–25; Pimari Chinchwad, India. p. 1–7. doi:10.1109/ASIANCON62057.2024.10837800.
90. Patil S, Kadam S, Katti J. Security enhancement of forensic evidences using blockchain. In: 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV); 2021 Feb 4–6; Tirunelveli, India. doi:10.1109/ICICV50876.2021.9388486.
91. Sangekar A, Gumalwad V, Khillare S, Warbhog K, Hadbe S, Tupe U. Blockchain-powered forensic evidence storage: a new approach to data security. In: 2024 IEEE Pune Section International Conference (PuneCon); 2024 Dec 13–15; Pune, India. doi:10.1109/PuneCon63413.2024.10895214.
92. Yap HP, Ong WL, Koh J, Liu H, Yang T, Chen Z. AI-based approach to efficient information extraction for supply chain contracts. In: 2024 IEEE Conference on Artificial Intelligence (CAI); 2024 Jun 25–27; Singapore. doi:10.1109/CAI59869.2024.00034.
93. Tassel P, Kovács B, Gebser M, Schekotihin K, Stöckermann P, Seidel G. Semiconductor fab scheduling with self-supervised and reinforcement learning. In: 2023 Winter Simulation Conference (WSC); 2023 Dec 10–13; San Antonio, TX, USA. p. 1924–35. doi:10.1109/WSC60868.2023.10407747.
94. Kaur I, Kumar Y, Sandhu AK. A comprehensive survey of AI, blockchain technology and big data applications in medical field and global health. In: 2021 International Conference on Technological Advancements and Innovations (ICTAI); 2021 Nov 10–12; Tashkent, Uzbekistan. doi:10.1109/ictai53825.2021.9673285.
95. Subbarao C, Saidamma B, Narasimha Raju PV, Srinivas C, Varghese IK, Shiva B. Role of block chain technology in improving security and efficiency in pharmaceutical supply chains. In: 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI); 2024 Aug 28–30; Coimbatore, India. doi:10.1109/ICoICI62503.2024.10696562.
96. Kumar R, Tripathi R. Traceability of counterfeit medicine supply chain through blockchain. In: Proceedings of the 2019 11th International Conference on COMSNETS; 2019 Jan 7–11; Bengaluru, India. p. 393–7.
97. Kulkarni A, Vijayakumar V, Nikam D, Patil A, Siddavatam API. Enhancing pharmaceutical security: SecureMeds-a robust drug traceability platform. In: 2024 2nd International Conference on Advancement in Computation & Computer Technologies (InCACCT); 2024 May 2–3; Gharuan, India. doi:10.1109/InCACCT61598.2024.10550976.
98. D'souza S, Nazareth D, Vaz C, Shetty M. Blockchain and AI in pharmaceutical supply chain. In: Proceedings of the International Conference on Smart Data Intelligence (ICSMDI 2021); 2021 Apr 29–30; Trichy, India. p. 1–14.
99. Ghadge A, Bourlakis M, Kamble S, Seuring S. Blockchain implementation in pharmaceutical supply chains: a review and conceptual framework. *Int J Prod Res.* 2023;61(19):6633–51. doi:10.1080/00207543.2022.2125595.
100. Kuruvilla JM, Kathrine GJW, Kirubakaran SS, Prem Prasad G, Evangelina G. Implementation of industry 4.0 in supply chain management in the healthcare industry. In: 2023 2nd International Conference on Edge Computing and Applications (ICECAA); 2023 Jul 19–21; Namakkal, India. doi:10.1109/ICECAA58104.2023.10212417.
101. Silva-Aravena F, Ceballos-Fuentealba I, Álvarez-Miranda E. Inventory management at a Chilean hospital pharmacy: case study of a dynamic decision-aid tool. *Mathematics.* 2020;8(11):1962. doi:10.3390/math8111962.
102. Zhang P, Liu X, Li W, Yu X. Pharmaceutical cold chain management based on blockchain and deep learning. *J Internet Technol.* 2021;22(7):1531–42. doi:10.53106/160792642021122207007.
103. Arora M, Saini JR, Sharma M, Kaparwan R, Pant M, Samanta P. Securing the cold chain with blockchain technology: from traceability to trust. In: 2025 International Conference on Intelligent Control, Computing and Communications (IC3); 2025 Feb 13–14; Mathura, India. doi:10.1109/IC363308.2025.10956450.
104. Jossy ST, Jossy SL, Joseph D, Elappila M, Kumar S. Smart storage solutions for cold chain: integrating technology for vaccine preservation. In: 2024 12th International Conference on Intelligent Systems and Embedded Design (ISED); 2024 Dec 20–22; Rourkela, India. doi:10.1109/ISED63599.2024.10956312.

105. Shanthi P, Venkatesh K. Blockchain assisted Archimedes optimization with machine learning driven drug supply management for pharmaceutical sector. In: 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI); 2023 May 25–26; Chennai, India. doi:10.1109/ACCAI58221.2023.10199884.
106. Anu SM, Kumar MS, Shankarmma, Chaithra M, Meghana K, Sanvi HR. Blockchain-powered authentication and supply chain integration to combat counterfeit drugs. In: 2024 5th International Conference on Circuits, Control, Communication and Computing (I4C); 2024 Oct 4–5; Bangalore, India. doi:10.1109/I4C62240.2024.10748485.
107. Gupta R, Shukla A, Tanwar S. BATS: a blockchain and AI-empowered drone-assisted telesurgery system towards 6G. *IEEE Trans Netw Sci Eng.* 2021;8(4):2958–67. doi:10.1109/TNSE.2020.3043262.
108. Ahalawat K, Tiwari R, Sharma A, Rawat N, Gupta P. Technological transformation in e-pharmacy: a bibliometric insight into healthcare advancements. In: 2025 International Conference on Ambient Intelligence in Health Care (ICAHC); 2025 Jan 10–11; Raipur Chattisgarh, India. doi:10.1109/ICAHC64101.2025.10956677.
109. Mondal S, Das S, Golder SS, Bose R, Sutradhar S, Mondal H. AI-driven big data analytics for personalized medicine in healthcare: integrating federated learning, blockchain, and quantum computing. In: 2024 International Conference on Artificial Intelligence and Quantum Computation-Based Sensor Application (ICAQSA); 2024 Dec 20–21; Nagpur, India. doi:10.1109/ICAQSA64000.2024.10882330.
110. Pisirgen A, Hizioglu OA. Applications of digital twin in precision medicine: a systematic review. In: 2025 International Conference on New Trends in Computing Sciences (ICTCS); 2025 Apr 16–18; Amman, Jordan. doi:10.1109/ICTCS65341.2025.10989480.
111. Rana MT, Numan M, Yousif M, Hussain T, Khan AZ, Zhao X. Enhancing sustainability in electric mobility: exploring blockchain applications for secure EV charging and energy management. *Comput Electr Eng.* 2024;119:109503. doi:10.1016/j.compeleceng.2024.109503.
112. Chen Z, Sarkis J, Yildizbasi A. Digital transformation for safer circular lithium-ion battery supply chains: a blockchain ecosystem-data perspective. *Int J Prod Res.* 2025;63(5):1585–606. doi:10.1080/00207543.2024.2381224.
113. Gohil K, Gohil A, Gupta R, Tanwar S. Deep learning and proxy smart contract-based supply chain management for electric vehicles. In: 2024 IEEE Third International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES); 2024 Apr 26–28; Delhi, India. doi:10.1109/icpeices62430.2024.10719230.
114. Mugurusi G, Ahishakiye E. Blockchain technology needs for sustainable mineral supply chains: a framework for responsible sourcing of Cobalt. *Procedia Comput Sci.* 2022;200:638–47. doi:10.1016/j.procs.2022.01.262.
115. Wessel J, Schoo A, Kwade A, Herrmann C. Traceability in battery cell production. *Energy Technol.* 2023;11(5):2200911. doi:10.1002/ente.202200911.
116. Antônio Rufino C Jr, Sanseverino ER, Gallo P, Koch D, Schweiger HG, Zanin H. Blockchain review for battery supply chain monitoring and battery trading. *Renew Sustain Energy Rev.* 2022;157:112078. doi:10.1016/j.rser.2022.112078.
117. Ribeiro da Silva E, Lohmer J, Rohla M, Angelis J. Unleashing the circular economy in the electric vehicle battery supply chain: a case study on data sharing and blockchain potential. *Resour Conserv Recycl.* 2023;193:106969. doi:10.1016/j.resconrec.2023.106969.
118. Choudhary D, Sangwan KS, Singh A. Blockchain-enabled architecture for lead acid battery circularity. *Sci Rep.* 2024;14:16467. doi:10.1038/s41598-024-67404-z.
119. Ananthanarayanan Bragadeesh S, Umamakeswari A. Secured vehicle life cycle tracking using blockchain and smart contract. *Comput Syst Sci Eng.* 2022;41(1):1–18. doi:10.32604/csse.2022.019842.
120. Arunmozhi M, Venkatesh VG, Arisian S, Shi Y, Raja Sreedharan V. Application of blockchain and smart contracts in autonomous vehicle supply chains: an experimental design. *Transp Res Part E Logist Transp Rev.* 2022;165:102864. doi:10.1016/j.tre.2022.102864.
121. Cheng ZQ, Dong Y, Shi A, Liu W, Hu Y, O'Connor J, et al. SHIELD: LLM-driven schema induction for predictive analytics in EV battery supply chain disruptions. In: Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing: Industry Track; 2024 Nov 12–16; Miami, FL, USA. Stroudsburg, PA, USA: Association for Computational Linguistics; 2024. doi:10.18653/v1/2024.emnlp-industry.24.

122. Banerjee A, Pawar DS, Kalambe M. Artificial intelligence in supply chain management for automobile industry. *Ind Eng J.* 2024;53(3):114–26.
123. Vasantha C, Mayank J, Agrawal A, Mondal A. Intelligent algorithm for optimizing delivery time in electric vehicle fleet systems. In: 2025 17th International Conference on Communication Systems and Networks (COMSNETS); 2025 Jan 6–10; Bengaluru, India. p. 156–61. doi:10.1109/COMSNETS63942.2025.10885593.
124. Dorokhova M, Vianin J, Alder JM, Ballif C, Wyrsh N, Wannier D. A blockchain-supported framework for charging management of electric vehicles. *Energies.* 2021;14(21):7144. doi:10.3390/en14217144.
125. Al-Saif N, Ahmad RW, Salah K, Yaqoob I, Jayaraman R, Omar M. Blockchain for electric vehicles energy trading: requirements, opportunities, and challenges. *IEEE Access.* 2021;9:156947–61. doi:10.1109/ACCESS.2021.3130095.
126. Garg S, Kaur K, Kaddoum G, Gagnon F, Rodrigues JJPC. An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment. In: 2019 IEEE International Conference on Communications Workshops (ICC Workshops); 2019 May 20–24; Shanghai, China. doi:10.1109/iccw.2019.8756952.
127. Martyushev NV, Malozyomov BV, Demin AY, Pogrebnoy AV, Efremenkov EA, Valuev DV, et al. Modeling the reliability of an electric car battery while changing its charging and discharge characteristics. *Mathematics.* 2025;13(11):1832. doi:10.3390/math13111832.
128. Indushree PS, Kiranmayi GR, Sundar SS. An inclusive survey of Internet of vehicles with emphasis on cyber security & forensics. In: 2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS); 2023 Dec 14–15; Chennai, India. doi:10.1109/ICCEBS58601.2023.10449092.
129. World Economic Forum. Redesigning trust: blockchain deployment toolkit—data integrity. Geneva, Switzerland: World Economic Forum; 2020 [cited 2025 May 1]. Available from: https://widergets.weforum.org/blockchain-toolkit/data-integrity/index.html?utm_source=chatgpt.com.
130. MIT Center for Transportation & Logistics. A consensus on the truth? Blockchain applications in supply chain management. MIT CTL supply chain exchange roundtable report; 2018 Oct 9–10. [cited 2025 May 1]. Available from: https://ctl.mit.edu/sites/ctl.mit.edu/files/2020-09/MIT_CTL_Blockchain_Rountable_Supply_Chain_Management.pdf.
131. Idrissi ZK, Lachgar M, Hrimech H. Blockchain, IoT and AI in logistics and transportation: a systematic review. *Transp Econ Manag.* 2024;2:275–85. doi:10.1016/j.team.2024.09.002.
132. Alzahrani B, Oubbati OS, Barnawi A, Atiquzzaman M, Alghazzawi D. UAV assistance paradigm: state-of-the-art in applications and challenges. *J Netw Comput Appl.* 2020;166:102706. doi:10.1016/j.jnca.2020.102706.
133. Hawashin D, Nemer M, Salah K, Jayaraman R, Svetinovic D, Damiani E. Blockchain and NFT-based traceability and certification for UAV parts in manufacturing. *J Ind Inf Integr.* 2024;39:100597. doi:10.1016/j.jii.2024.100597.
134. Aggarwal S, Kumar N, Tanwar S. Blockchain-envisioned UAV communication using 6G networks: open issues, use cases, and future directions. *IEEE Internet Things J.* 2021;8(7):5416–41. doi:10.1109/JIOT.2020.3020819.
135. Alkadi R, Alnuaimi N, Yeun CY, Shoufan A. Blockchain interoperability in unmanned aerial vehicles networks: state-of-the-art and open issues. *IEEE Access.* 2022;10:14463–79. doi:10.1109/ACCESS.2022.3145199.
136. Satheesh Kumar M, Vimal S, Jhanjhi NZ, Dhanabalan SS, Alhumyani HA. Blockchain based peer to peer communication in autonomous drone operation. *Energy Rep.* 2021;7:7925–39. doi:10.1016/j.egyr.2021.08.073.
137. Hashemi SM, Ali Hashemi S, Botez RM, Ghazi G. A novel fault-tolerant air traffic management methodology using autoencoder and P2P blockchain consensus protocol. *Aerospace.* 2023;10(4):357. doi:10.3390/aerospace10040357.
138. Fernández-Caramés TM, Blanco-Novoa O, Froiz-Míguez I, Fraga-Lamas P. Towards an autonomous industry 4.0 warehouse: a UAV and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. *Sensors.* 2019;19(10):2394. doi:10.3390/s19102394.
139. Hafeez S, Shawky MA, Al-Quraan M, Mohjazi L, Ali Imran M, Sun Y. BETA-UAV: blockchain-based efficient authentication for secure UAV communication. *arXiv:2402.15817.* 2024.
140. Islam A, Young S. A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. *Comput Electr Eng.* 2020;84(3):106627. doi:10.1016/j.compeleceng.2020.106627.
141. Collins E, Wang M. Federated learning: a survey on privacy-preserving collaborative intelligence. *arXiv:2504.17703.* 2025.

142. Feng C, Liu B, Yu K, Goudos SK, Wan S. Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs. *IEEE Trans Ind Inform.* 2022;18(5):3582–92. doi:10.1109/TII.2021.3116132.
143. Ferrag MA, Friha O, Maglaras L, Janicke H, Shu L. Federated deep learning for cyber security in the Internet of Things: concepts, applications, and experimental analysis. *IEEE Access.* 2021;9:138509–42. doi:10.1109/ACCESS.2021.3118642.
144. Zhu C, Zhu X, Ren J, Qin T. Blockchain-enabled federated learning for UAV edge computing network: issues and solutions. *IEEE Access.* 2022;10:56591–610. doi:10.1109/ACCESS.2022.3174865.
145. Gupta R, Kumari A, Tanwar S. Fusion of blockchain and artificial intelligence for secure drone networking underlying 5G communications. *Trans Emerg Telecommun Technol.* 2021;32(1):e4176. doi:10.1002/ett.4176.
146. Xiao W, Li M, Alzahrani B, Alotaibi R, Barnawi A, Ai Q. A blockchain-based secure crowd monitoring system using UAV swarm. *IEEE Netw.* 2021;35(1):108–15. doi:10.1109/MNET.011.2000210.
147. He Y, Hu R, Liang K, Liu Y, Zhou Z. Deep reinforcement learning algorithm with long short-term memory network for optimizing unmanned aerial vehicle information transmission. *Mathematics.* 2025;13(1):46. doi:10.3390/math13010046.
148. Howard J. The humanoid 100: mapping the humanoid robot value chain [Internet]. New York, NY, USA: Morgan Stanley; 2023 [cited 2025 May 23]. Available from: https://advisor.morganstanley.com/john.howard/documents/field/j/jo/john-howard/The_Humanoid_100_-_Mapping_the_Humanoid_Robot_Value_Chain.pdf.
149. Keshvarparast A, Battini D, Battaia O, Pirayesh A. Collaborative robots in manufacturing and assembly systems: literature review and future research agenda. *J Intell Manuf.* 2024;35(5):2065–118. doi:10.1007/s10845-023-02137-w.
150. Patel AR, Azadi S, Babaee MH, Mollaei N, Patel KL, Mehta DR. Significance of robotics in manufacturing, energy, goods and transport sector in Internet of Things (IoT) paradigm. In: 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA); 2018 Aug 16–18; Pune, India. p. 1–4. doi:10.1109/ICCUBEA.2018.8697488.
151. Bernardo R, Sousa JMC, Gonçalves PJS. Survey on robotic systems for internal logistics. *J Manuf Syst.* 2022;65:339–50. doi:10.1016/j.jmsy.2022.09.014.
152. Fernandes M, Alexandre LA. RobotChain: artificial intelligence on a blockchain using Tezos technology. *Ledger.* 2019;4(S1):32–41. doi:10.5195/ledger.2019.175.
153. Lopes V, Alexandre LA. Detecting robotic anomalies using RobotChain. In: 2019 IEEE International Conference on Autonomous Robot Systems and Competitions (ICARSC); 2019 Apr 24–26; Porto, Portugal. p. 1–6. doi:10.1109/icarsc.2019.8733618.
154. Lopes V, Pereira N, Alexandre LA. Robot workspace monitoring using a blockchain-based 3D vision approach. In: 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW); 2019 Jun 16–17; Long Beach, CA, USA. p. 2812–20. doi:10.1109/cvprw.2019.00340.
155. Lopes V, Pereira N, Fernandes M, Alexandre LA. A time-segmented consortium blockchain for robotic event registration. In: Proceedings of the 2021 3rd International Conference on Blockchain Technology; 2021 Mar 26–28; Shanghai, China. p. 117–22. doi:10.1145/3460537.3460557.
156. Castelló Ferrer E, Rudovic O, Hardjono T, Pentland AS. RoboChain: a secure data-sharing framework for human-robot interaction. In: Proceedings of the 10th International Conference on eHealth, Telemedicine, and Social Medicine (eTELEMED); 2018 Mar 25–29; Rome, Italy. p. 24–9.
157. Castelló Ferrer E. The blockchain: a new framework for robotic swarm systems. *arXiv:1608.00695.* 2016. doi:10.48550/arxiv.1608.00695.
158. Castelló Ferrer E, Hardjono T, Dorigo M, Pentland AS. Secure and secret cooperation in robotic swarms. *arXiv:1904.09266.* 2019. doi:10.48550/arxiv.1904.09266.
159. Peña Queralta J, Westerlund T. Blockchain-powered collaboration in heterogeneous swarms of robots. In: Proceedings of the 2020 IEEE International Conference on Industrial Cyber-Physical Systems (ICPS); 2020 Jun 9–12; Tampere, Finland. p. 169–74.

160. Pacheco A, Strobel V, Dorigo M. A blockchain-controlled physical robot swarm communicating via an *ad-hoc* network. In: Dorigo M, Birattari M, Blum C, Christensen AL, Reina A, Garnier S, editors. Swarm intelligence. Berlin/Heidelberg, Germany: Springer; 2020. p. 3–15. doi:10.1007/978-3-030-60376-2_1.
161. Nawaz A, Wang L, Irfan M, Westerlund T. Hyperledger sawtooth based supply chain traceability system for counterfeit drugs. Comput Ind Eng. 2024;190:110021. doi:10.1016/j.cie.2024.110021.
162. Hassini M, Redondo-Iglesias E, Venet P. Battery passports for second-life batteries: an experimental assessment of suitability for mobile applications. Batteries. 2024;10(5):153. doi:10.3390/batteries10050153.
163. Ajakwe SO, Igboanusi IS, Lee JM, Kim DS. iBANDA: a blockchain-assisted defense system for authentication in drone-based logistics. Drones. 2025;9(8):590. doi:10.3390/drones9080590.
164. Tang Y, Zhang Y, Niu T, Li Z, Zhang Z, Chen H, et al. A survey on blockchain-based federated learning: categorization, application and analysis. Comput Model Eng Sci. 2024;139(3):2451–77. doi:10.32604/cmesci.2024.030084.