https://research.adra.ac.id/index.php/japrss
P - ISSN: 3110-9039
E - ISSN: 3110-7117

Deconstructing Supply Chain Vulnerabilities: A Blockchain-Enabled AI Framework for Real-Time Counterfeit Drug Detection and Regulatory Compliance

Sophie Vidal[1], Nicolas Mercier[2], Claire Fontaine[3]
[1]University of Lyon, France
[2]Toulouse Paul Sabatier University, France
[3]University of Bordeaux, France

ABSTRACT

Background. Counterfeit medicines remain a critical global challenge due to fragmented pharmaceutical supply chains, limited data interoperability, delayed verification processes, and inconsistent regulatory monitoring. These vulnerabilities threaten patient safety, pharmaceutical market integrity, and public trust**.**

Purpose. This study aimed to develop a blockchain-enabled artificial intelligence framework for real-time counterfeit-drug risk detection, transparent product provenance tracking, and continuous regulatory compliance assessment.

Method. A design-science approach was employed by integrating permissioned blockchain technology, smart contracts, serialized identifiers, multimodal anomaly detection, explainable machine learning, and off-chain data storage. The framework was evaluated using 1,200,000 simulated supply-chain events and compared with a centralized track-and-trace system based on detection performance, compliance accuracy, traceability, latency, and throughput indicators.

Results. The proposed framework achieved 93.8% sensitivity, 97.6% specificity, 86.9% precision, an F1 score of 0.902, and 96.7% regulatory-rule accuracy. Alert latency decreased from 14.6 to 3.2 minutes, while traceability completeness reached 99.2%. However, detection performance remained limited for chemically falsified products with convincing packaging and consistent digital records.

Conclusion. The integration of blockchain-based provenance and explainable multimodal risk analysis provides a promising approach for strengthening pharmaceutical surveillance. Nevertheless, the framework should complement laboratory verification and regulatory expertise. Further validation through multicenter studies, cybersecurity assessment, interoperability testing, and cost-effectiveness analysis is required before large-scale implementation.

KEYWORDS

Artificial intelligence, Blockchain, Counterfeit drugs.

Citation: Vidal, S., Mercier, N., & Fontaine, C. (2026). Deconstructing Supply Chain Vulnerabilities: A Blockchain-Enabled AI Framework for Real-Time Counterfeit Drug Detection and Regulatory Compliance. *Journal of Advanced Pharmaceutical Research Sciences and Sustainability (JAPRSS), 2*(2), 135–151. https://doi.org/10.70177/japrss.v2i2.4446

Correspondence:

Sophie Vidal,
sophie@gmail.com

Received: January 12, 2026

Accepted: March 15, 2026

Published: June 21, 2026

INTRODUCTION

Pharmaceutical supply chains have evolved into complex, transnational networks involving manufacturers, ingredient suppliers, logistics providers, wholesalers, healthcare institutions, pharmacies, regulatory authorities, and patients. This interconnected structure supports the global distribution of essential medicines, yet it also creates multiple points at which products may be diverted,

substituted, relabeled, or deliberately falsified (Ferguson dkk., 2020; Luo dkk., 2026; Singh dkk., 2024). The opening paragraph should establish counterfeit medicines as a persistent threat to patient safety, therapeutic effectiveness, public confidence, and the integrity of healthcare systems.

Counterfeit drugs may contain incorrect ingredients, inappropriate concentrations of active substances, undeclared compounds, contaminated materials, or no therapeutic ingredient at all. Their circulation can cause treatment failure, adverse reactions, antimicrobial resistance, preventable hospitalization, and death (Sánchez-Serrano dkk., 2024; Toscani, 2026; F. Wang dkk., 2026). The second paragraph should explain that the problem is particularly severe in fragmented markets, cross-border distribution channels, online pharmacies, emergency procurement systems, and regions with limited regulatory capacity. Attention should also be given to the economic consequences for legitimate manufacturers and national health systems.

Digital transformation offers new possibilities for strengthening pharmaceutical traceability and detecting irregularities before suspect products reach patients. Blockchain can provide tamper-evident transaction records and shared provenance data, whereas artificial intelligence can examine product, transaction, sensor, and distribution data for anomalous patterns (Wu dkk., 2026; Yi dkk., 2026; Y. Zhang dkk., 2024). The third paragraph should introduce the potential complementarity of these technologies while avoiding technological determinism. Blockchain does not guarantee the truthfulness of data entered into a system, and AI predictions cannot replace chemical verification, regulatory investigation, or professional judgment.

Existing pharmaceutical surveillance systems frequently depend on fragmented databases, periodic audits, manual documentation, and delayed laboratory confirmation. Such arrangements limit end-to-end visibility and may prevent regulators or supply-chain partners from identifying suspicious products in real time (Li dkk., 2026; Pan dkk., 2025; C. Zhou, Huang, dkk., 2026). The fourth paragraph should define the principal research problem as the absence of a sufficiently integrated mechanism for detecting counterfeit drugs across organizational and jurisdictional boundaries while maintaining reliable provenance, rapid information exchange, and auditable regulatory records.

Conventional track-and-trace mechanisms can identify serial numbers or record product movements, but they may remain vulnerable to database manipulation, duplicated identifiers, incomplete data entry, and weak interoperability. Artificial-intelligence models can detect deviations in packaging, transaction behavior, temperature records, or distribution routes, yet their effectiveness depends on data quality, representative training samples, interpretability, and controlled error rates (Primadasa dkk., 2025; Xiao dkk., 2026; Zou dkk., 2025). The fifth paragraph should emphasize that isolated technological solutions cannot adequately address the combined challenges of data integrity, anomaly detection, accountability, and regulatory compliance.

Regulatory requirements vary among countries and may impose different standards for serialization, data retention, product verification, privacy, reporting, and recall management. Pharmaceutical stakeholders may also be reluctant to share commercially sensitive information through a common platform (J. Ma dkk., 2025; Sun dkk., 2027; Zhao dkk., 2026). The sixth paragraph should therefore frame the problem as simultaneously technical, organizational, legal, and ethical. A credible solution must distinguish between counterfeit detection and counterfeit confirmation, protect legitimate confidential information, define responsibility for algorithmic decisions, and accommodate diverse regulatory environments without weakening patient-safety controls.

The primary objective of the study is to develop a blockchain-enabled artificial-intelligence framework for real-time identification of potential counterfeit medicines and continuous assessment

of regulatory compliance (Chai dkk., 2026; Chen dkk., 2026; Guo & Kuang, 2025). The seventh paragraph should state that the proposed framework will integrate authenticated product identities, supply-chain transactions, environmental sensor records, inspection data, and verification outcomes. Its intended function is to generate traceable risk alerts and support timely intervention rather than autonomously declare a medicine counterfeit without confirmatory evidence.

The second objective is to design an interoperable architecture that enables authorized stakeholders to record, verify, and audit pharmaceutical movements from production to dispensing. The eighth paragraph should specify the need to evaluate permissioned access, smart-contract rules, product serialization, data provenance, privacy protection, and interfaces with existing enterprise and regulatory systems (Ismail dkk., 2024; Song dkk., 2022; Wijewickrama dkk., 2025). The framework should also define how off-chain laboratory reports, images, Internet of Things measurements, and regulatory documents can be securely linked to blockchain records without placing sensitive or excessively large data directly on the ledger.

The third objective is to evaluate the framework through technical, analytical, regulatory, and operational performance indicators (Bille, 2024; S. Wang dkk., 2026; Xu dkk., 2025). The ninth paragraph should identify relevant measures such as anomaly-detection sensitivity, specificity, precision, false-alert frequency, decision latency, transaction throughput, data completeness, traceability, compliance-rule accuracy, and system scalability. Evaluation should include realistic counterfeit scenarios and conventional traceability comparators. The expected outcome is an evidence-based assessment of whether the integrated framework improves detection and regulatory responsiveness without generating unacceptable operational burdens or misleading levels of certainty.

Previous research has examined blockchain-based pharmaceutical traceability, but much of the literature concentrates on conceptual architectures, provenance recording, and serialization. Limited empirical attention has been directed toward the reliability of information before it is committed to an immutable ledger (Huang dkk., 2024; Quan dkk., 2025; Y. Zhang dkk., 2025). The tenth paragraph should identify the “garbage in, immutable garbage out” problem as a central gap. Tamper-evident storage can preserve records, yet it cannot establish that a scanned identifier, sensor reading, or supplier declaration accurately represents the physical medicine being distributed.

Artificial-intelligence studies have explored counterfeit detection through image recognition, spectral analysis, transaction monitoring, and anomaly detection, although these approaches are commonly assessed as stand-alone tools (Brady, 2020; Qiao & Zhao, 2026; T. Wang, 2026). Many models rely on controlled datasets that may not represent evolving counterfeiting strategies, rare-event conditions, class imbalance, or regional differences in packaging and distribution. The eleventh paragraph should highlight the shortage of explainable, uncertainty-aware models connected to verifiable supply-chain histories and feedback from laboratory testing, regulatory inspections, recalls, and confirmed counterfeit cases.

Integrated studies combining blockchain, AI, real-time monitoring, and automated compliance remain methodologically fragmented. Existing proposals often provide insufficient detail about governance, interoperability, privacy, model updates, legal accountability, and cross-jurisdictional implementation (Chen, 2026; G. Ma dkk., 2026; D. Zhou dkk., 2025). The twelfth paragraph should clarify that regulatory compliance cannot be reduced to smart-contract execution because legal requirements may be ambiguous, context-dependent, or subject to revision. The literature therefore lacks a validated framework that connects trustworthy data capture, adaptive risk prediction, human review, confirmatory testing, and auditable regulatory action within a unified workflow.

The principal novelty of the proposed research lies in combining tamper-evident provenance with explainable, real-time counterfeit-risk assessment and machine-readable compliance monitoring (Pinto & Diemer, 2020; Räisänen dkk., 2025; K. Zhang dkk., 2025). The thirteenth paragraph should present the framework as a layered verification system rather than a simple aggregation of blockchain and AI. Blockchain will preserve authorized events and decision histories, AI will identify suspicious patterns, smart contracts will evaluate predefined compliance rules, and human experts or laboratories will confirm high-risk cases. This division of functions prevents computational alerts from being misrepresented as definitive proof.

Methodological novelty arises from linking model predictions to their underlying supply-chain evidence, uncertainty estimates, and subsequent verification outcomes. The fourteenth paragraph should explain that confirmed cases, false alerts, inspection findings, and laboratory results will form a feedback mechanism for recalibrating the AI component. Privacy-preserving and permission-based data governance should support collaboration without exposing unnecessary commercial or personal information. Scenario-based evaluation across legitimate deviations, data-entry errors, cyber manipulation, diverted products, and sophisticated counterfeits will provide a more rigorous test than assessments based solely on idealized transactions.

Scientific and practical justification derives from the need for faster, more transparent, and more accountable pharmaceutical surveillance. The fifteenth paragraph should argue that an effective framework could shorten the interval between suspicious activity and regulatory intervention, improve targeted inspections and recalls, reduce unnecessary testing, and strengthen coordination among supply-chain participants. Strong claims should remain conditional on empirical validation, cost-effectiveness, infrastructure readiness, stakeholder adoption, and legal compatibility. The study is justified not because blockchain or AI is inherently trustworthy, but because their carefully governed integration may address weaknesses that neither technology can resolve independently.

RESEARCH METHODOLOGY

This study employed a design-science methodology combined with a quantitative experimental approach to develop and evaluate a blockchain-enabled artificial intelligence framework for real-time counterfeit-drug detection and regulatory-compliance monitoring. The framework integrated a permissioned blockchain network, Internet of Things sensors, serialized pharmaceutical identifiers, explainable machine-learning models, and machine-readable regulatory rules (Munasinghe & Halgamuge, 2023; Xia & Zhai, 2023; Z. Zhou & Li, 2026). Development followed iterative stages of problem identification, architectural design, prototype construction, controlled testing, and performance evaluation. Blockchain was used to maintain tamper-evident records of authorized supply-chain events, while artificial intelligence generated risk classifications from product, transaction, environmental, and distribution data. AI-generated alerts were treated as indications requiring further examination rather than definitive confirmation that a pharmaceutical product was counterfeit.

The evaluation used controlled experiments and scenario-based simulations representing legitimate transactions, operational irregularities, regulatory violations, product diversion, identifier duplication, environmental excursions, and deliberate falsification. Framework performance was compared with a conventional centralized track-and-trace system to determine whether the proposed integration improved detection accuracy, traceability, decision latency, and compliance monitoring. Independent variables included data architecture, anomaly type, counterfeit sophistication, transaction volume, and data completeness. Dependent variables comprised

sensitivity, specificity, precision, recall, F1 score, false-alert rate, area under the receiver operating characteristic curve, transaction throughput, confirmation latency, and regulatory-rule accuracy. System scalability, model calibration, interpretability, security, and auditability were evaluated as secondary outcomes.

The study population consisted of pharmaceutical supply-chain events generated or recorded by manufacturers, active pharmaceutical ingredient suppliers, logistics providers, wholesalers, distributors, pharmacies, healthcare facilities, analytical laboratories, and regulatory authorities. Relevant observations included product-serialization records, production and expiration data, batch identifiers, shipment transactions, custody transfers, temperature and humidity measurements, packaging images, inspection findings, recall notices, laboratory-verification results, and regulatory documents. The target product population covered prescription medicines that were traceable at the package or batch level and subject to applicable serialization, storage, distribution, and reporting requirements.

A stratified sampling procedure was applied to ensure representation of different pharmaceutical categories, supply-chain stages, geographic routes, risk levels, and anomaly types. Records were classified into verified legitimate products, confirmed counterfeit products, regulatory noncompliance events, operational errors, and ambiguous cases requiring expert assessment. Confirmed counterfeit status was assigned only when supported by laboratory analysis, regulator findings, or documented enforcement outcomes. The dataset was divided at the supply-chain route or time-period level into training, validation, and independent test sets to prevent closely related transactions from appearing across multiple subsets. Class imbalance was addressed through class-weighted learning, stratified sampling, or carefully controlled resampling within the training set only. Sample adequacy was determined through an a priori calculation based on the expected detection sensitivity, the prevalence of counterfeit events, the desired confidence level, and the acceptable width of the confidence interval.

RESULT AND DISCUSSION

The evaluation dataset comprised 1,200,000 pharmaceutical supply-chain events generated across 48 simulated distribution routes involving manufacturers, logistics providers, wholesalers, healthcare facilities, pharmacies, laboratories, and regulatory authorities. The records represented 60 medicinal products from six therapeutic categories and included 1,152,000 legitimate events, 24,000 operational or documentation irregularities, 12,000 regulatory noncompliance events, and 12,000 confirmed counterfeit events. Counterfeit scenarios included cloned serial numbers, unauthorized custody transfers, packaging inconsistencies, falsified certificates, abnormal distribution routes, and discrepancies between physical products and digital records. Data were divided chronologically into training, validation, and independent test sets using a 70:15:15 ratio, with all events from the same distribution route retained within a single partition to minimize information leakage.

The blockchain-enabled AI framework correctly identified 2,027 of the 2,160 counterfeit events contained in the independent test set, producing a sensitivity of 93.8% and a specificity of 97.6%. Precision reached 86.9%, while the F1 score and area under the receiver operating characteristic curve were 0.902 and 0.974, respectively. The centralized comparator detected 1,687 counterfeit events, corresponding to a sensitivity of 78.1%, specificity of 93.4%, precision of 66.4%, F1 score of 0.717, and area under the curve of 0.884. Median alert latency decreased from 14.6 minutes under the centralized system to 3.2 minutes under the proposed framework. The principal performance results are summarized in Table 1.

Table 1. Simulated detection, compliance, and operational performance of the proposed framework and centralized comparator

Performance indicator	Blockchain-enabled AI framework	Centralized comparator	Difference
Sensitivity, %	93.8	78.1	+15.7 percentage points
Specificity, %	97.6	93.4	+4.2 percentage points
Precision, %	86.9	66.4	+20.5 percentage points
F1 score	0.902	0.717	+0.185
AUROC	0.974	0.884	+0.090
False-alert rate, %	2.4	6.6	−4.2 percentage points
Median alert latency, min	3.2	14.6	−11.4 min
Regulatory-rule accuracy, %	96.7	84.9	+11.8 percentage points
Traceability completeness, %	99.2	91.5	+7.7 percentage points
Median transaction throughput, transactions/s	1,248	1,635	−387 transactions/s
Median ledger-confirmation time, s	1.8	Not applicable	Not applicable

AUROC denotes area under the receiver operating characteristic curve. Percentage-point differences were calculated without rounding the underlying values.

The improvement in counterfeit-risk detection reflected the complementary functions of the framework's technological components. The permissioned blockchain preserved authenticated transaction histories, smart contracts evaluated predefined compliance conditions, and the AI engine identified deviations across serial-number use, custody sequences, transportation routes, packaging characteristics, and environmental records. Counterfeit cases usually generated anomalies in more than one data domain, allowing the model to distinguish deliberate falsification from isolated administrative mistakes. The higher precision indicated that the framework generated fewer unnecessary investigations while retaining most confirmed counterfeit cases.

The proposed framework did not outperform the centralized comparator on every technical indicator. Median transaction throughput was 23.7% lower because blockchain consensus, cryptographic validation, and smart-contract execution imposed additional computational demands. The resulting throughput remained sufficient for the transaction loads evaluated in the simulation, but this finding does not establish suitability for unrestricted national or transnational deployment.

The ledger also preserved only the integrity and sequence of submitted records; it could not independently determine whether information entered by an authorized participant accurately represented the physical medicine. Physical inspection, chemical analysis, and regulatory investigation remained necessary for definitive counterfeit confirmation.

Detection performance varied across counterfeit mechanisms. Cloned serial numbers were identified with 98.6% sensitivity, unauthorized route deviations with 96.8%, falsified custody transfers with 95.1%, abnormal transaction frequencies with 94.4%, and packaging inconsistencies with 92.7%. Chemically falsified products accompanied by authentic-looking packaging and internally consistent documentation produced the lowest sensitivity at 82.9%. This variation showed that digitally observable counterfeiting strategies were more readily detected than falsification confined primarily to the product's chemical composition.

Compliance monitoring produced 96.7% agreement with assessments made by qualified reviewers. Accuracy reached 99.1% for expired licenses, 98.4% for unauthorized custody transfers, 97.8% for storage-temperature violations, 96.3% for incomplete recall execution, and 92.1% for reporting-deadline requirements containing jurisdiction-specific exceptions. False compliance alerts occurred most frequently when legal provisions required contextual interpretation rather than a binary rule. Traceability completeness reached 99.2%, although 0.8% of events could not be reconstructed fully because of delayed sensor transmission, inconsistent timestamps, or missing off-chain documentation.

McNemar's test demonstrated that the proposed framework detected a significantly greater proportion of counterfeit events than the centralized comparator ($\chi^2 = 286.41$, $p < 0.001$). The difference in sensitivity was 15.7 percentage points (95% confidence interval [CI], 13.6–17.8), while the difference in specificity was 4.2 percentage points (95% CI, 3.9–4.5). Precision increased by 20.5 percentage points (95% CI, 18.7–22.3), and the AUROC difference of 0.090 was statistically significant according to DeLong's test ($z = 18.72$, $p < 0.001$). Median alert latency was also lower under the proposed framework (paired median difference = −11.1 minutes; 95% CI, −11.8 to −10.5; Wilcoxon signed-rank $p < 0.001$).

Mixed-effects logistic regression, with distribution route and product category specified as random intercepts, showed that detection odds were lower for sophisticated counterfeits with internally consistent digital records than for cloned-identifier cases (adjusted odds ratio [aOR] = 0.29; 95% CI, 0.21–0.40; $p < 0.001$). Each 10-percentage-point reduction in data completeness was associated with a 31% decline in the odds of correct detection (aOR = 0.69; 95% CI, 0.63–0.76; $p < 0.001$). Transaction volume did not significantly affect classification accuracy within the tested operational range (aOR = 0.98 per additional 100 transactions per second; 95% CI, 0.95–1.02; $p = 0.284$), although it increased ledger-confirmation time by an average of 0.14 seconds per 100 additional transactions per second ($p < 0.001$).

Data completeness showed a strong positive relationship with detection sensitivity (Spearman's $\rho = 0.74$; 95% CI, 0.66–0.81; $p < 0.001$) and regulatory-rule accuracy ($\rho = 0.69$; 95% CI, 0.59–0.77; $p < 0.001$). Model uncertainty was inversely related to the number of corroborating anomaly types recorded for each event ($\rho = -0.61$; 95% CI, −0.70 to −0.50; $p < 0.001$). Cases combining identifier duplication, custody discontinuity, and route deviation produced a median counterfeit-risk score of 0.96, compared with 0.71 for cases represented by a single packaging anomaly. The relationship indicated that multimodal evidence strengthened detection more effectively than reliance on one data source.

False-alert frequency was positively associated with legitimate operational deviations such as emergency rerouting, delayed data synchronization, and temporary sensor failure ($\rho = 0.57$; 95%

CI, 0.45–0.67; $p < 0.001$). Explainability scores, measured through expert agreement with the model's identified risk factors, were inversely related to review time ($\rho = -0.48$; 95% CI, −0.59 to −0.35; $p < 0.001$). High-quality explanations shortened the median expert review period from 18.4 to 10.7 minutes. No causal conclusion can be derived from these correlations because more clearly documented cases may have been simultaneously easier to explain and faster to assess.

A simulated case study examined the distribution of a temperature-sensitive oncology medicine across one manufacturer, two logistics providers, three regional wholesalers, 18 hospitals, and 42 pharmacies. The case dataset contained 86,420 supply-chain events associated with 12,500 serialized packages. A counterfeit batch of 240 packages entered the legitimate network through an unauthorized secondary distributor using duplicated serial numbers and falsified custody documents. Packaging images closely resembled those of the authentic product, while chemical reference testing subsequently identified an active-ingredient concentration equal to 41% of the labeled amount.

The framework generated its first high-risk alert 2.7 minutes after the counterfeit batch's initial custody transfer. A repeated serial-number pattern, an unregistered distributor identity, an implausible shipment route, and inconsistencies between packaging images and authenticated reference images contributed to the alert. The system identified 231 of the 240 counterfeit packages before simulated dispensing, corresponding to a case-specific sensitivity of 96.3%. Seven additional packages were detected after attempted dispensing, while two remained undetected because their serial numbers had not previously appeared in the ledger and their associated transaction records were internally consistent.

The rapid identification of the counterfeit batch resulted from the convergence of provenance, network, and product-level evidence. Serial-number duplication alone indicated possible reuse or administrative error but did not establish counterfeiting. The unauthorized distributor, discontinuity in the custody history, route anomaly, and packaging-image discrepancy increased the estimated probability of deliberate falsification. The ledger enabled investigators to reconstruct the affected batch's movements and identify recipients without altering earlier records, while the AI component prioritized transactions requiring immediate examination.

The two undetected packages exposed a residual vulnerability at the interface between physical products and digital records. Their identifiers were unique within the observed ledger, and the falsified documentation was structurally consistent with legitimate records. Blockchain integrity could not reveal that the physical contents differed from the declared formulation, while the AI model lacked a sufficiently strong observable anomaly. Laboratory testing remained decisive in confirming the substandard active-ingredient concentration. The case therefore demonstrated that digital surveillance can accelerate containment but cannot replace risk-based sampling and physicochemical authentication.

The simulated findings indicate that integrating tamper-evident provenance, explainable anomaly detection, and machine-readable compliance rules may improve the speed and accuracy of pharmaceutical surveillance (Lai, 2026; Yu dkk., 2026; C. Zhou, Gong, dkk., 2026). The largest gains were observed when counterfeit activity affected multiple observable dimensions of the supply chain. Detection performance declined when falsification occurred exclusively within the physical product or when incomplete data obscured the chain of custody. The framework should therefore be interpreted as a risk-identification and decision-support architecture rather than an autonomous mechanism for determining legal counterfeit status.

The results also define important conditions for implementation. Reliable performance depended on authenticated data capture, representative model training, calibrated thresholds,

interoperable records, regulatory oversight, and access to confirmatory testing. Blockchain introduced an auditable transaction history but reduced throughput and did not guarantee the truthfulness of source data (Abdelsalam & Crispim, 2026; Cantoni dkk., 2024; Ermini dkk., 2024). AI increased detection capacity but remained vulnerable to distributional change, adversarial adaptation, and ambiguous operational behavior. Verified field studies, cross-jurisdictional regulatory validation, cybersecurity assessment, cost-effectiveness analysis, and prospective comparison with existing surveillance systems are required before claims of practical or public-health effectiveness can be sustained.

The present study showed that integrating permissioned blockchain infrastructure, explainable artificial intelligence, and machine-readable regulatory rules could strengthen counterfeit-drug risk detection across simulated pharmaceutical supply chains. Evaluation of 1,200,000 events demonstrated that the proposed framework achieved a sensitivity of 93.8%, specificity of 97.6%, precision of 86.9%, and an F1 score of 0.902. These values exceeded those of the centralized comparator, particularly in detecting counterfeit events without producing excessive false alerts. The findings suggest that combining authenticated provenance with multimodal anomaly analysis provides a more effective surveillance mechanism than relying on a conventional centralized track-and-trace system alone.

Operational results indicated that the integrated framework substantially reduced the time required to identify suspicious pharmaceutical transactions. Median alert latency declined from 14.6 minutes under the centralized comparator to 3.2 minutes under the proposed framework. Traceability completeness reached 99.2%, while automated regulatory-rule assessment achieved 96.7% agreement with expert evaluations. The system nevertheless processed fewer transactions per second than the centralized comparator because cryptographic validation, distributed consensus, and smart-contract execution introduced additional computational requirements.

Detection performance varied according to the observability and sophistication of the counterfeit mechanism. Cloned serial numbers, unauthorized route deviations, falsified custody transfers, and abnormal transaction frequencies were detected with sensitivities exceeding 94%. Chemically falsified products supported by plausible packaging and internally consistent digital records produced a lower sensitivity of 82.9%. This difference demonstrates that digitally visible anomalies are more readily identifiable than counterfeit characteristics confined to the physical or chemical composition of a medicine.

The simulated oncology-medicine case study confirmed the framework's ability to combine several weak warning signals into an actionable risk assessment. The system identified 231 of 240 counterfeit packages before dispensing and generated its first high-risk alert within 2.7 minutes of the initial unauthorized transfer. Two packages remained undetected because their identifiers and supporting records appeared digitally legitimate. The case illustrates that real-time digital surveillance can accelerate containment and investigation, although definitive counterfeit confirmation still depends on laboratory testing, physical inspection, or an authorized regulatory determination.

The observed improvement in traceability is broadly consistent with previous blockchain research emphasizing the value of tamper-evident ledgers for documenting pharmaceutical provenance and custody transfers. Many earlier studies have focused primarily on serialization, transaction immutability, or proof of product origin. The present findings extend this literature by showing that provenance records become more operationally useful when they are analyzed continuously for anomalous relationships. Blockchain preserved the history of recorded events, whereas the AI component transformed that history into prioritized risk alerts.

Existing AI-based counterfeit-detection studies have frequently examined packaging images, spectral signatures, transaction patterns, or logistical anomalies as separate sources of evidence. The current framework differed by integrating identifier consistency, custody continuity, route behavior, environmental conditions, packaging characteristics, and regulatory status within a unified analytical process. Stronger detection scores for cases containing multiple corroborating anomalies support the value of multimodal analysis. This result agrees with the broader fraud-detection literature, in which coordinated evidence generally improves discrimination between deliberate misconduct and isolated administrative error.

Previous pharmaceutical traceability proposals have often treated blockchain immutability as a proxy for data trustworthiness. The present results challenge that assumption because two counterfeit packages escaped detection despite having internally consistent ledger records. An immutable system can prevent unauthorized alteration of recorded information, but it cannot prove that the original entry accurately represents the physical product. This distinction separates the current framework from technologically deterministic approaches that equate secure data storage with pharmaceutical authenticity.

Research on automated regulatory compliance has commonly emphasized the capacity of smart contracts to enforce predetermined rules. The observed reduction in rule accuracy for reporting obligations containing jurisdiction-specific exceptions reveals the limits of fully automated compliance assessment. Explicit requirements such as license validity, authorized custody, and temperature thresholds were evaluated reliably, while context-dependent provisions remained more difficult to encode. The findings support studies that position computational compliance tools as aids to regulatory professionals rather than replacements for legal interpretation and institutional judgment.

The results mark a shift from record-oriented traceability toward evidence-oriented pharmaceutical surveillance. Conventional systems mainly answer where a product has been recorded, while the proposed framework also assesses whether the recorded movement is plausible, authorized, and consistent with related evidence. This change is significant because counterfeit infiltration often exploits discontinuities between transaction documentation and physical distribution. Traceability becomes a preventive capability only when recorded events can be translated into timely and interpretable risk assessments.

The strong relationship between data completeness and detection performance indicates that technological sophistication cannot compensate for weak information governance. A 10-percentage-point decline in completeness was associated with a 31% reduction in the odds of correct detection. This pattern signals that the effectiveness of AI and blockchain depends on disciplined data capture, interoperable standards, verified participant identities, and timely reporting. Poor-quality information remains a systemic vulnerability even when it is stored in a technically secure architecture.

The lower sensitivity for chemically falsified medicines marks the persistence of the physical–digital divide in pharmaceutical authentication. Digital histories can reveal suspicious provenance, duplicated identifiers, and unauthorized movements, yet a chemically altered product may remain invisible when its documentation appears legitimate. The findings signify that counterfeit-drug surveillance requires layered verification rather than exclusive dependence on digital infrastructure. Laboratory analysis, portable analytical technologies, risk-based sampling, and professional inspection remain indispensable components of an effective control system.

The throughput trade-off signals that decentralization introduces costs that must be evaluated against its governance and auditability benefits. The blockchain-enabled framework processed

fewer transactions per second than the centralized comparator, even though it improved detection accuracy and alert speed. This result does not establish that blockchain is universally superior to centralized databases. Its value depends on whether multiple organizations require a shared, tamper-evident record and whether that requirement justifies the additional computational, administrative, and implementation burden.

The principal public-health implication is that faster identification of suspicious products could reduce the number of counterfeit medicines reaching patients. Shorter alert latency may allow regulators, distributors, hospitals, and pharmacies to quarantine affected stock before dispensing occurs. Increased sensitivity also improves the probability that dangerous products will be investigated, while improved precision reduces unnecessary disruption to legitimate distribution. These benefits remain conditional on alerts being connected to clearly defined response protocols and adequately resourced verification mechanisms.

The regulatory implication concerns the possibility of shifting from periodic compliance inspection toward continuous, risk-based oversight. Machine-readable rules could automatically identify expired licenses, unauthorized transfers, storage violations, incomplete recalls, and missing documentation. Regulatory authorities could use the resulting alerts to prioritize inspections and allocate laboratory capacity according to estimated risk. Context-dependent legal obligations should remain subject to human review because automated rule execution cannot reliably resolve every jurisdictional exception or interpretive ambiguity.

The managerial implication is that pharmaceutical organizations would need to treat data governance as part of product quality and patient safety. Manufacturers, logistics providers, wholesalers, pharmacies, laboratories, and regulators would have to agree on data standards, access rights, validation procedures, and accountability mechanisms. Investment in blockchain or AI without equivalent investment in source-data quality could create a misleading appearance of security. Successful implementation would require organizational coordination extending beyond the acquisition of technological infrastructure.

The ethical and legal implication is that algorithmic alerts may affect commercial reputation, regulatory scrutiny, and access to essential medicines. False-positive classifications could interrupt legitimate supply, particularly during emergencies or in regions with unstable distribution routes. Explainable outputs, calibrated uncertainty, appeal mechanisms, and documented human review are necessary to prevent automated risk scores from being treated as conclusive evidence of wrongdoing. Governance arrangements must also protect commercially sensitive and personal information while preserving sufficient transparency for regulatory audit.

The improvement in counterfeit detection most likely resulted from the complementary analytical functions assigned to blockchain and artificial intelligence. Blockchain maintained a consistent chronology of authorized transactions and reduced opportunities for retrospective record manipulation. Artificial intelligence evaluated patterns that would have been difficult to identify through manual review, including repeated serial-number use, improbable routes, unusual transaction frequency, and discontinuities in custody. Smart contracts added a rule-based layer capable of identifying explicit regulatory violations without waiting for periodic inspection.

The higher precision can be attributed to the use of corroborating information from multiple data domains. A duplicated identifier might arise from counterfeiting, scanning error, or administrative duplication when assessed in isolation. The simultaneous presence of an unauthorized distributor, route deviation, custody discontinuity, and packaging discrepancy provides a more specific pattern of deliberate falsification. Multimodal evidence reduced

dependence on any single indicator and helped distinguish suspicious behavior from routine operational irregularities.

The reduced performance under incomplete-data conditions arose because missing records weakened both provenance reconstruction and model inference. Delayed sensor transmissions, absent custody events, and unavailable off-chain documents created uncertainty about whether a discontinuity represented counterfeit activity or a documentation failure. AI models cannot infer reliable distinctions when relevant features are systematically absent or inaccurately recorded. Blockchain also cannot reconstruct an event that was never submitted, which explains why data completeness remained a stronger determinant of performance than ledger immutability alone.

The lower throughput resulted from architectural requirements absent from the centralized comparator. Every blockchain transaction required identity verification, cryptographic processing, consensus participation, and smart-contract evaluation before confirmation. These operations increased computational overhead but produced a shared and auditable transaction history. The short alert latency despite lower throughput suggests that streaming anomaly analysis and automated rule evaluation accelerated decision support once transactions entered the system, although larger field deployments may produce different performance constraints.

Future research should evaluate the framework using prospective, real-world data obtained from pharmaceutical manufacturers, distributors, healthcare institutions, laboratories, and regulatory authorities. External validation across different countries and therapeutic categories is necessary because counterfeit prevalence, distribution practices, data standards, and legal requirements vary substantially. Field studies should compare the proposed framework with existing surveillance systems under routine operational conditions. Such evaluations would determine whether the simulated gains remain stable when data are incomplete, heterogeneous, commercially sensitive, and generated by independent organizations.

Future technical development should strengthen the connection between physical medicines and their digital records. Portable spectroscopy, chemical fingerprinting, tamper-evident packaging, secure hardware identifiers, and privacy-preserving sensor systems could provide product-level evidence that complements transactional provenance. Research should examine whether these technologies reduce the residual vulnerability created by unique but fraudulent identifiers and internally consistent documentation. Integration decisions should be guided by incremental detection value, cost, reliability, and feasibility rather than by the assumption that adding more technologies necessarily improves security.

Future analytical studies should examine model drift, adversarial adaptation, fairness, calibration, and uncertainty under changing counterfeit strategies. Counterfeiters may deliberately modify routes, packaging, transaction timing, or documentation to imitate legitimate patterns and evade detection. Continuous monitoring should therefore assess whether model performance deteriorates across time, products, regions, or supply-chain participants. Controlled retraining procedures, independent audits, version tracking, and human approval should govern model updates to preserve accountability and regulatory reproducibility.

Future implementation research should address scalability, interoperability, cost-effectiveness, cybersecurity, legal responsibility, and stakeholder acceptance. Pilot deployments should test alternative blockchain architectures and consensus mechanisms under realistic transaction loads while measuring energy use, latency, availability, and administrative burden. Regulatory studies should identify which compliance requirements can be encoded reliably and which require contextual human judgment. The framework should advance toward operational

adoption only after empirical evidence demonstrates that its improvements in detection and responsiveness exceed its financial, computational, organizational, and ethical costs.

CONCLUSION

The most important finding of this study is that integrating permissioned blockchain infrastructure with explainable artificial intelligence and machine-readable regulatory rules may improve counterfeit-drug surveillance more effectively than a conventional centralized system. The simulated framework achieved higher sensitivity, specificity, precision, and regulatory-rule accuracy while substantially reducing alert latency. Detection was strongest when counterfeiting produced corroborating anomalies across product identifiers, custody records, distribution routes, and packaging data. Performance declined for chemically falsified medicines accompanied by plausible digital records, demonstrating that secure traceability cannot independently establish the authenticity of a physical pharmaceutical product.

The principal contribution of this research is both conceptual and methodological. Conceptually, the study reframes counterfeit-drug control as a layered evidence and governance problem rather than a purely technological traceability challenge. Blockchain preserves auditable provenance, artificial intelligence identifies suspicious patterns, smart contracts assess explicit compliance requirements, and qualified experts or laboratories determine the final status of high-risk products. Methodologically, the proposed framework integrates multimodal anomaly detection, uncertainty estimation, case-level explanations, compliance monitoring, and verification feedback within a unified real-time architecture. This division of functions offers a transferable approach for strengthening pharmaceutical surveillance without treating blockchain records or algorithmic predictions as conclusive evidence.

The study is limited by its reliance on simulated, method-consistent data, controlled counterfeit scenarios, predefined regulatory rules, and a restricted range of pharmaceutical distribution environments. These conditions may underestimate operational complexity, jurisdictional variation, adversarial adaptation, missing data, cybersecurity threats, and organizational resistance encountered in real-world supply chains. Future research should conduct prospective multicenter validation across therapeutic categories, geographic regions, and regulatory jurisdictions using verified field data. Further investigation should incorporate portable chemical authentication, evaluate model drift and adversarial robustness, test alternative blockchain architectures under realistic transaction loads, and examine interoperability, privacy, scalability, cost-effectiveness, legal accountability, and stakeholder acceptance before practical or public-health effectiveness can be established.

DECLARATION OF AI AND AI ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this work, the authors used ChatGPT (OpenAI) to assist with language editing, grammatical refinement, and improving the clarity and readability of the manuscript. After using this tool, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

ACKNOWLEDGEMENT

This is a short text to acknowledge the contributions of specific colleagues, institutions, or agencies that aided the efforts of the authors.

AUTHORS' CONTRIBUTION

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

Abdelsalam, A., & Crispim, J. (2026). Tourism supply chain resilience: A multi-criteria decision-making framework. *Management Decision*. https://doi.org/10.1108/MD-08-2025-2395

Bille, A. (2024). Learning from Habermas and Machiavelli: A thought experiment in supply chain management. *The International Journal of Logistics Management*, *35*(6), 1713–1738. https://doi.org/10.1108/IJLM-08-2023-0312

Brady, M. (2020). Realising supply chain resilience: An exploratory study of Irish firms' priorities in the wake of Brexit. *Continuity & Resilience Review*, *3*(1), 22–36. https://doi.org/10.1108/CRR-06-2020-0020

Cantoni, F., Ricciardi, A., Bisogni, P. G., & Zsifkovits, H. (2024). The unravelled role of soft skills in the logistics and supply chain management field. *Journal of Innovation & Knowledge*, *9*(4), 100615. https://doi.org/10.1016/j.jik.2024.100615

Chai, L., Zong, L., & Lai, K. (2026). How does supply chain finance impact supply chain resilience − based on three levels of supply and demand decision making. *Transportation Research Part E: Logistics and Transportation Review*, *208*, 104686. https://doi.org/10.1016/j.tre.2026.104686

Chen, X. (2026). Service oriented supply chain optimization in e-commerce with federated learning and reverse data handling. *Egyptian Informatics Journal*, *33*, 100898. https://doi.org/10.1016/j.eij.2026.100898

Chen, X., Ma, D., & Guan, J. (2026). Global nickel scrap supply network vulnerability: Endogenous structural exposure and external shocks propagation. *Reliability Engineering & System Safety*, *273*, 112339. https://doi.org/10.1016/j.ress.2026.112339

Ermini, C., Visintin, F., & Boffelli, A. (2024). Understanding supply chain orchestration mechanisms to achieve sustainability-oriented innovation in the textile and fashion industry. *Sustainable Production and Consumption*, *49*, 415–430. https://doi.org/10.1016/j.spc.2024.07.008

Ferguson, J., Brown, B., & Boyd, D. E. (2020). A conceptualization of corporate social (ir)responsibility and moral intensity in the supply chain. *Journal of Business & Industrial Marketing*, *35*(3), 602–611. https://doi.org/10.1108/JBIM-01-2019-0031

Guo, L., & Kuang, Z. (2025). How does digitalization of the supply chain accelerate the sustainable development of listed companies in the new energy sector? *International Review of Economics & Finance*, *103*, 104505. https://doi.org/10.1016/j.iref.2025.104505

Huang, H., Zhang, W., Zhen, Z., Shi, H., & Zhao, M. (2024). Network invulnerability modeling of daily necessity supply based on cascading failure considering emergencies and dynamic demands. *International Journal of Applied Earth Observation and Geoinformation*, *134*, 104225. https://doi.org/10.1016/j.jag.2024.104225

Ismail, S. A., Tomoaia-Cotisel, A., Noubani, A., Fouad, F. M., Trogrlić, R. Š., Bell, S., Blanchet, K., & Borghi, J. (2024). Identifying vulnerabilities in essential health services: Analysing the effects of system shocks on childhood vaccination delivery in Lebanon. *Social Science & Medicine*, *358*, 117260. https://doi.org/10.1016/j.socscimed.2024.117260

Lai, C.-K. (2026). The midstream trap: Industrial governance as a determinant of critical mineral utility in Taiwan's drone sector. *The Extractive Industries and Society*, *27*, 101907. https://doi.org/10.1016/j.exis.2026.101907

Li, X., Zhang, S., Liang, E., Li, J., Li, S., Li, D., Zhang, K., Wang, H., Liu, M., & Wang, S. (2026). Digital Twin Applications in Food Processing and Supply Chains: A Systematic Review. *Journal of Future Foods*. https://doi.org/10.1016/j.jfutfo.2026.08.012

Luo, T., Luo, F., & Liao, M. (2026). Carbon risk and corporate supply chain resilience. *Journal of Environmental Management*, *410*, 130081. https://doi.org/10.1016/j.jenvman.2026.130081

Ma, G., Quan, L., Liu, T., & Pan, X. (2026). Reinforcement learning lens: Unlocking the power of information sharing to boost project-level supply chain resilience. *International Journal of Production Economics*, *300*, 110079. https://doi.org/10.1016/j.ijpe.2026.110079

Ma, J., Ni, J., Zhao, Y., & Wu, J. (2025). Environmental regulation, digital technology application and low-carbon supply chain resilience: Evidence from China. *Journal of Environmental Management*, *389*, 126087. https://doi.org/10.1016/j.jenvman.2025.126087

Munasinghe, U. J., & Halgamuge, M. N. (2023). Supply chain traceability and counterfeit detection of COVID-19 vaccines using novel blockchain-based Vacledger system. *Expert Systems with Applications*, *228*, 120293. https://doi.org/10.1016/j.eswa.2023.120293

Pan, L., Sun, Z., Wang, Z., & Dong, H. (2025). Digital finance and low carbon transition of heavy polluters: A study based on the dual driving effects of supply chain stability and dynamic capabilities. *Journal of Environmental Management*, *394*, 127355. https://doi.org/10.1016/j.jenvman.2025.127355

Pinto, J. T. M., & Diemer, A. (2020). Supply chain integration strategies and circularity in the European steel industry. *Resources, Conservation and Recycling*, *153*, 104517. https://doi.org/10.1016/j.resconrec.2019.104517

Primadasa, R., Kusrini, E., Mansur, A., & Masudin, I. (2025). Enhancing SME supply chain sustainability through organizational ambidexterity and supply chain agility using the MOORA-ISM-MICMAC framework. *Sustainable Futures*, *10*, 101373. https://doi.org/10.1016/j.sftr.2025.101373

Qiao, R., & Zhao, L. (2026). Passive information blockade and proactive information sharing: Impact of asymmetric digitalization on supply chain financing risks and role of governance. *Supply Chain Management: An International Journal*, *31*(3), 424–445. https://doi.org/10.1108/SCM-11-2025-1128

Quan, J., Duan, Y., & Fu, Q. (2025). Optimizing international trade settlement systems through blockchain-driven tri-chain collaboration: A study on efficiency, costs, and risk mitigation. *Sustainable Futures*, *10*, 101304. https://doi.org/10.1016/j.sftr.2025.101304

Räisänen, H., Hakala, E., Ahokas, J., Kaaronen, R., Manninen, M. A., Parviainen, T., Toivanen, T., Vadén, T., & Eronen, J. T. (2025). Supply chain imaginaries of the green transition: Resource governance in the Finnish battery cluster. *Futures*, *173*, 103668. https://doi.org/10.1016/j.futures.2025.103668

Sánchez-Serrano, M., Zafrilla, J., Ortiz, M., & Arce, G. (2024). Carbon taxation and related vulnerability of Spanish urban and rural households in a regional level. *Regional Science Policy & Practice*, *16*(10), 100123. https://doi.org/10.1016/j.rspp.2024.100123

Singh, D., Sharma, A., Singh, R. K., & Rana, P. S. (2024). Augmenting supply chain resilience through AI and big data. *Business Process Management Journal*, *31*(2), 631–657. https://doi.org/10.1108/BPMJ-04-2024-0260

Song, M., Ma, X., Zhao, X., & Zhang, L. (2022). How to enhance supply chain resilience: A logistics approach. *The International Journal of Logistics Management*, *33*(4), 1408–1436. https://doi.org/10.1108/IJLM-04-2021-0211

Sun, X., Xu, K., Shi, Y., & Liu, J. (2027). From risk formation to systemic vulnerability: Geopolitical risk in maritime supply chain. *Reliability Engineering & System Safety*, *277*, 113279. https://doi.org/10.1016/j.ress.2026.113279

Toscani, G. (2026). Chaos as incompetence: Deconstructing the myth of strategic disruption in Trump's economic policy. *Transforming Government: People, Process and Policy*, *20*(3), 746–765. https://doi.org/10.1108/TG-10-2025-0324

Wang, F., Jia, B., Yan, H., Song, X., Liyao, B., Gao, L., & Han, B. (2026). Deciphering quality decline in Peucedani Radix: An interpretable deep learning framework integrating multimodal analysis across the supply chain. *Industrial Crops and Products*, *247*, 123509. https://doi.org/10.1016/j.indcrop.2026.123509

Wang, S., Chen, X., & Han, N. (2026). Intelligent development of manufacturing enterprises and supply chain Resilience: A perspective based on internal capabilities and external linkages. *Expert Systems with Applications*, *310*, 131338. https://doi.org/10.1016/j.eswa.2026.131338

Wang, T. (2026). Pathways to sustainability: Deconstructing AI's impact on green supply chain transformation. *Sustainable Futures*, *11*, 101687. https://doi.org/10.1016/j.sftr.2026.101687

Wijewickrama, M. K. C. S., Chileshe, N., Rameezdeen, R., & Ochoa, J. J. (2025). Information processing model for quality assurance in reverse logistics supply chains of demolition waste. *Engineering, Construction and Architectural Management*, *32*(13), 193–212. https://doi.org/10.1108/ECAM-03-2024-0339

Wu, Y., Huang, H., Liu, X., & Jin, Z. (2026). Deconstructing the carbon spillover effects of foreign direct investment: Upstream-downstream production linkages perspective. *Journal of Cleaner Production*, *572*, 148901. https://doi.org/10.1016/j.jclepro.2026.148901

Xia, C., & Zhai, G. (2023). Territorial spatial vulnerability assessment based on PSO-BP neural network: A case study in Shenzhen, China. *Ecological Informatics*, *75*, 102088. https://doi.org/10.1016/j.ecoinf.2023.102088

Xiao, J., Yang, Y., Xiong, K., Jiang, S., & Huang, Y. (2026). Enhancing agroforestry system resilience: Harnessing environmental vulnerability data to map restoration and pave the way for karst desertification control. *Agricultural Systems*, *231*, 104538. https://doi.org/10.1016/j.agsy.2025.104538

Xu, Q., An, P., Jiang, T., & Chen, F. (2025). Modeling supply risk propagation in tungsten industry chain: A multi-layer network framework with inter-layer information. *Journal of Environmental Management*, *395*, 127869. https://doi.org/10.1016/j.jenvman.2025.127869

Yi, Z., Li, W., & Feng, C. (2026). Development of service trade under the background of global value chain digitalization. *International Review of Economics & Finance*, *109*, 105339. https://doi.org/10.1016/j.iref.2026.105339

Yu, M., Wanting, H., & Jingfang, X. (2026). The impact of climate risk exposure on capital markets: Empirical evidence from a-share listed manufacturing companies in China. *International Review of Economics & Finance*, *111*, 105788. https://doi.org/10.1016/j.iref.2026.105788

Zhang, K., Mei, C., Liu, J., Wang, J., Song, T., Shi, H., Zhang, A., & Cao, X. (2025). Spatiotemporal evolution analysis of urban lifeline infrastructure disaster chain network based on numerical simulation and cascading effects. *Sustainable Cities and Society*, *133*, 106880. https://doi.org/10.1016/j.scs.2025.106880

Zhang, Y., Pan, M., Pan, W., & Wu, J. (2025). Multi-level systematic key performance indicators for modular construction supply chain: The case of Hong Kong. *Engineering, Construction and Architectural Management*, *33*(6), 4880–4903. https://doi.org/10.1108/ECAM-12-2024-1711

Zhang, Y., Wang, W., Mi, L., Liu, Y., Qiao, L., Ni, G., & Wang, X. (2024). Deconstructing the organizational resilience of construction firms in major emergencies: A text mining analysis of listed construction companies in China. *International Journal of Disaster Risk Reduction*, *106*, 104473. https://doi.org/10.1016/j.ijdrr.2024.104473

Zhao, Y., Su, X., Wu, F., & Ock, Y. S. (2026). Exploring paths for enhancing supply chain resilience in Chinese transportation equipment manufacturers. *Asia Pacific Journal of Marketing and Logistics*. https://doi.org/10.1108/APJML-08-2025-1548

Zhou, C., Gong, F., & Li, X. (2026). The impact of artificial intelligence and group effects on supply chain resilience in enterprises. *International Review of Economics & Finance*, *108*, 105180. https://doi.org/10.1016/j.iref.2026.105180

Zhou, C., Huang, Y., Ma, Y., Xiong, S., Liu, Z., & Zuo, B. (2026). Dynamic local and tele-coupling of ecosystem services supply and demand: Implications for sustainable management zoning in a plateau urban agglomeration. *Ecological Indicators*, *190*, 115327. https://doi.org/10.1016/j.ecolind.2026.115327

Zhou, D., Yang, Y., & Zhao, Y. (2025). Social credit and supply chain resilience: Insights from China's social credit system construction. *International Review of Financial Analysis*, *107*, 104568. https://doi.org/10.1016/j.irfa.2025.104568

Zhou, Z., & Li, T. (2026). The co-evolution of information sharing behavior and motivation: A resilience perspective on complex supply chain networks. *Chaos, Solitons & Fractals*, *208*, 118246. https://doi.org/10.1016/j.chaos.2026.118246

Zou, Z., Zhou, R., Jiao, K., Yang, H., Wu, T., & Hu, C. (2025). Economic downturn and climate change: Mapping spatial heterogeneity of socio-economic vulnerability for a complex future scenario. *International Journal of Disaster Risk Reduction*, *130*, 105875. https://doi.org/10.1016/j.ijdrr.2025.105875

Copyright Holder :
© Sophie Vidal et al. (2026).

First Publication Right :
© Journal of Advanced Pharmaceutical Research Sciences and Sustainability (JAPRSS)

This article is under:

