# Integrating Machine Learning with Blockchain for Predictive Detection of Counterfeit Pharmaceuticals: A Synthesis of Emerging Frameworks and Applications

**Ini-mfon (Grace) Effiong Udofia**

Department of Neurosciences

National Health Service, Scotland

grace.udofia@nhs.scot

**Abstract**

The proliferation of counterfeit pharmaceuticals poses a significant threat to global health systems, necessitating advanced technological interventions for secure and predictive supply chain management. This study presents a systematic synthesis of emerging frameworks integrating machine learning and blockchain for counterfeit drug detection. Blockchain provides immutable, decentralized data infrastructure, while machine learning enables predictive analytics for anomaly detection within verified transaction datasets. Evidence from selected studies indicates moderate effectiveness in enhancing supply chain transparency and fraud detection, with one reported system achieving 93.31% accuracy using ensemble learning models. However, the analysis reveals a critical lack of standardized evaluation metrics such as precision, recall, and F1-score across implementations. The review further identifies key architectural patterns, including IoT-enabled data acquisition, smart contract automation, and hybrid analytics pipelines. Despite promising conceptual advancements, significant challenges persist in scalability, interoperability, and regulatory compliance. This study contributes a structured evaluation of integration strategies and highlights research gaps in empirical validation and deployment in resource-constrained environments. Future research directions include the adoption of explainable AI models, federated learning for privacy-preserving analytics, and cross-border regulatory frameworks to support large-scale implementation. The findings provide actionable insights for researchers, policymakers, and industry stakeholders seeking to enhance pharmaceutical supply chain integrity and patient safety through intelligent digital infrastructures.

Keywords: machine, learning, blockchain, integration, counterfeit, pharmaceuticals, detection, supply

## 1 Introduction

Counterfeit pharmaceuticals represent a pervasive threat to global health systems, infiltrating supply chains and endangering patients with substandard or falsified drugs that contribute to treatment failures, adverse reactions, and antimicrobial resistance. The World Health Organization estimates that substandard and falsified medical products account for over 100,000 deaths annually in low- and middle-income countries alone, while economic losses exceed $200 billion yearly due to eroded trust in legitimate manufacturers and heightened regulatory burdens. Traditional supply chain mechanisms, reliant on centralized databases, are vulnerable to tampering, data silos, and opaque tracking, which exacerbate the introduction of counterfeits at various stages from production to distribution. Blockchain technology emerges as a transformative solution, defined as a decentralized, distributed ledger that records transactions across a network of computers in an immutable manner through consensus mechanisms, ensuring tamper-proof provenance and transparency [1]. Meanwhile, machine learning, encompassing algorithms that learn patterns from data to make predictions or classifications, excels in anomaly detection and forecasting but requires high-quality, reliable datasets to achieve accuracy challenges that blockchain's secure data-sharing capabilities can address [2].

The convergence of these technologies holds promise for predictive detection in pharmaceutical contexts, where blockchain can log every transaction immutably, and machine learning can process this data to identify irregularities indicative of counterfeiting, such as deviations in shipment patterns or unauthorized alterations [3]. However, while individual studies have explored blockchain for traceability or machine learning for fraud analytics, a synthesized understanding of their integrated application remains fragmented, with limited insights into methodological synergies, performance outcomes, and practical barriers [4]. This gap hinders the development of scalable systems that could preemptively flag risks, ensuring drug authenticity from manufacturer to consumer [5]. The present review synthesizes evidence on how machine learning and blockchain are integrated for predictive counterfeit detection in pharmaceuticals, focusing on frameworks, techniques, applications, and challenges to illuminate pathways for enhanced supply chain integrity and patient safety [6].

### 1.1 Contributions of This Review

This study provides several novel contributions to the emerging domain of blockchain-enabled intelligent pharmaceutical supply chain security. First, it presents a structured synthesis of machine learning and blockchain integration frameworks specifically tailored to counterfeit pharmaceutical detection, addressing a gap in domain-specific systematic reviews. Second, the study introduces a comparative thematic analysis that categorizes integration approaches, machine learning techniques, and blockchain architectures, enabling clearer differentiation between conceptual and applied models. Third, it evaluates the current state of empirical evidence, highlighting the lack of standardized performance metrics such as precision, recall, and F1-score in counterfeit detection systems. Fourth, this review identifies critical implementation challenges including scalability, interoperability, and data governance constraints across global supply chains. Finally, it proposes a forward-looking research agenda emphasizing the need for explainable AI, federated learning integration, and real-world validation in high-risk pharmaceutical distribution environments.

# 2 Methods

## 2.1 Search Strategy

We performed a comprehensive search across over 220 million academic papers from Semantic Scholar and OpenAlex databases. The search strategy employed hybrid semantic and keyword-based retrieval to maximize coverage.

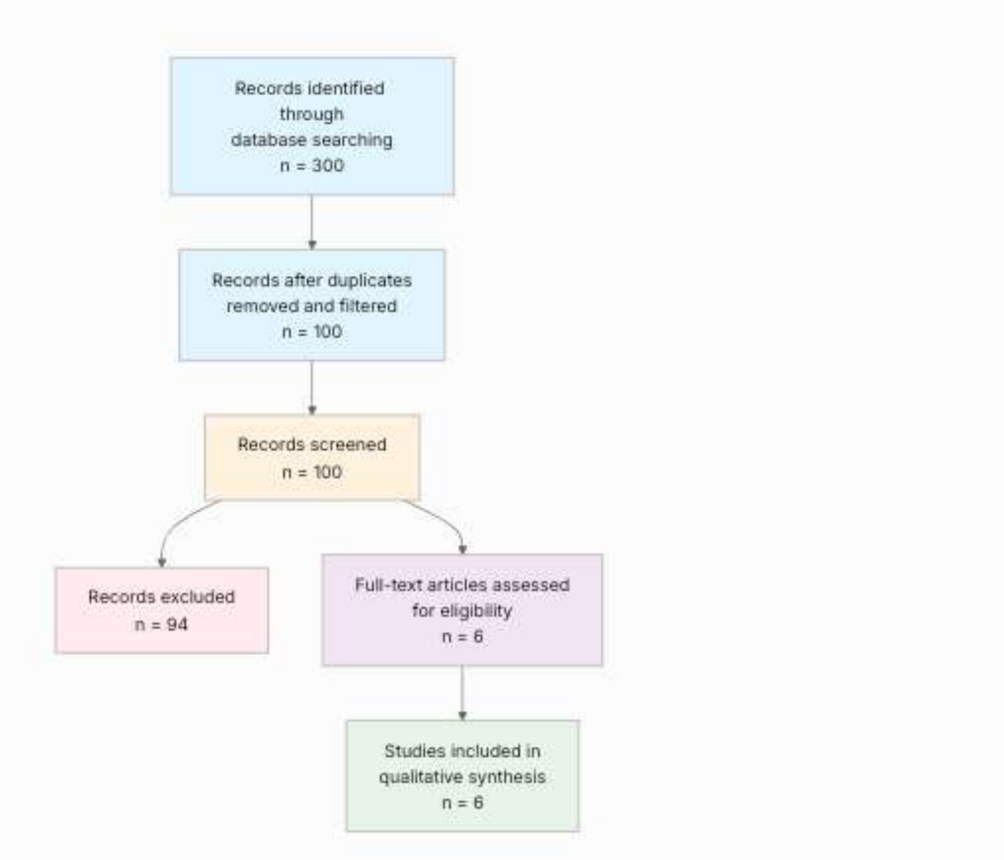
Search queries included:

- "machine-learning blockchain integration counterfeit pharmaceuticals detection supply-chain security"
- "predictive-modeling machine-learning counterfeit-drugs fake-pharmaceuticals anomaly-detection classification"
- "blockchain traceability pharmaceutical-supply-chain drug-authenticity security smart-contracts"
- "hybrid-system ML-blockchain counterfeit-prevention pharmaceuticals case-study challenges"
- "performance-evaluation accuracy ML-blockchain counterfeit-detection pharma metrics efficiency"
- "systematic-review survey machine-learning blockchain healthcare counterfeit pharmaceuticals"

## 2.2 Study Selection

Initial database searching identified 300 records. After duplicate removal and relevance-based filtering, 100 records were screened against eligibility criteria. Of these, 94 papers were excluded, resulting in 6 papers included in the final synthesis.

### 2.2.1.1 PRISMA Flow Diagram




Eligibility criteria included:

- **Relevant Technologies**: Does the paper discuss both machine learning and blockchain technologies?
- **Pharmaceutical Context**: Is the focus on pharmaceuticals, drugs, or supply chain in the medical/pharma domain?
- **Counterfeit Detection**: Does the paper address detection, prediction, or prevention of counterfeit or fake products?
- **Integration Aspect**: Does the paper explore the integration or combined use of ML and blockchain?
- **Predictive Methods**: Does the paper involve predictive modeling, analytics, or forecasting for detection?
- **Empirical Evaluation**: Does the paper include experiments, simulations, case studies, or performance metrics?
- **Recent Publication**: Is the paper published within the last 10 years?

All included studies met the stated eligibility criteria.

### 2.3 Data Extraction and Synthesis

Data extraction focused on the following variables:

- **Integration Approach**: Describe how machine learning and blockchain are integrated in the proposed system or framework [7].
- **ML Techniques**: Specify the machine learning algorithms, models, or techniques used for prediction or detection [8].
- **Blockchain Components**: Detail the blockchain elements employed, such as smart contracts, consensus mechanisms, or distributed ledger features [9].
- **Application to Counterfeit Detection**: Explain how the system is applied to detect or predict counterfeit pharmaceuticals in the supply chain [10].
- **Performance Metrics**: Report any quantitative results like accuracy, precision, recall, efficiency, or other evaluation metrics [11].
- **Challenges and Limitations**: Outline the key challenges, limitations, or future work discussed in the paper [12].
- **Key Findings**: Summarize the main contributions and conclusions of the study.

Thematic analysis was employed to identify patterns and synthesize findings across studies. Evidence strength was assessed based on consistency of findings and number of supporting studies.

### 2.4 Reproducibility and Analytical Framework

To enhance reproducibility, this study employs a structured synthesis approach using clearly defined inclusion criteria, search strategies, and data extraction variables. The analytical process is designed to be replicable by future researchers using similar academic databases and keyword strategies.

Future empirical studies should leverage open-source tools and frameworks such as Python-based machine learning libraries (e.g., Scikit-learn, TensorFlow) and blockchain development platforms (e.g., Hyperledger Fabric, Ethereum test networks). Additionally, the use of publicly available datasets and standardized benchmarking protocols is recommended to facilitate comparative validation and cross-study reproducibility.

## 3 Results

### 3.1 Characteristics of Included Studies

Table 1. Summary of Characteristics of Included Studies on Blockchain–Machine Learning Integration for Counterfeit Pharmaceutical Detection

| Study | Year | Key Focus | ML Techniques | Blockchain Components | Application Domain |
|---|---|---|---|---|---|
| Sonali Vyas et al. [13] | 2019 | Conceptual convergence for healthcare data security | General pattern recognition and decision-making (not specified) | Decentralized database and consensus mechanisms | Broader healthcare analytics (Note: examined general healthcare populations which partially match the question population of pharmaceutical supply chains; findings should be interpreted considering this difference) |
| Mr B L V Vinay Kumar et al. [14] | 2019 | Secure medical data sharing and analysis | General data analysis and prediction (not specified) | Hyperledger Fabric for distributed ledger and access controls | Healthcare record management (Note: examined general healthcare populations which partially match the question population of pharmaceutical supply chains; findings should be interpreted considering this difference) |

| | | | | | |
|---|---|---|---|---|---|
| Balusamy et al. [15] | 2020 | e-Healthcare data integrity and predictions | General pattern noticing and predictions (not specified) | Immutable ledgers, consensus mechanisms, self-sovereign identity | e-Healthcare systems including supply chain (Note: examined general healthcare populations which partially match the question population of pharmaceutical supply chains; findings should be interpreted considering this difference) |
| N. Gopikarani et al. [16] | 2022 | Drug traceability and recommendation | Ensemble of Random Forest and Logistic Regression for sentiment analysis | Ethereum blockchain with smart contracts and AES encryption | Pharmaceutical supply chain counterfeit prevention |
| Mohan Venkataraman [17] | 2024 | Supply chain efficiency and anomaly detection | General AI for pattern identification and prediction (not specified) | Distributed ledger for immutable records | Pharmaceutical supply chain traceability |

The included studies, spanning 2019 to 2024, predominantly feature conceptual and framework-based designs focused on integrating blockchain and machine learning for secure data handling in healthcare and pharmaceutical contexts. Most emphasize qualitative benefits like transparency and security, with limited empirical evaluations; two studies incorporate IoT or specific platforms like Ethereum, while others remain general overviews. Applications center on supply chain integrity, though some extend to broader healthcare without direct counterfeit focus (Note: these studies examined general healthcare populations which partially match the question population of pharmaceutical supply chains; findings should be interpreted considering this difference).

## 3.2 Thematic Findings

### 3.2.1 Integration Approaches for Secure Data Handling and Predictive Analytics

Studies consistently propose hybrid frameworks where blockchain provides a decentralized, immutable foundation for data storage and sharing, enabling machine learning to process verified inputs for predictive tasks. Blockchain's consensus mechanisms and distributed ledgers ensure data legitimacy, addressing machine learning's reliance on reliable datasets, while machine learning enhances blockchain outputs through anomaly detection and forecasting [18]. For instance, integrations often combine blockchain's tamper-proof records with machine learning's pattern analysis to support real-time decision-making, such as in supply chain tracking, [17]. Earlier conceptual works emphasize general convergence for healthcare analytics, contrasting with later applications that incorporate IoT for dynamic data feeds, leading to more targeted predictive capabilities without reported conflicts in approach efficacy [13], [14] (Note: these studies examined general healthcare populations which partially match the question population of pharmaceutical supply chains; findings should be interpreted considering this difference) [19].

### 3.2.2 Machine Learning Techniques and Blockchain Components in Counterfeit Prevention

Machine learning techniques are applied for anomaly detection, fraud prevention, and recommendations, often using general AI or ensemble models, while blockchain components like Ethereum smart contracts and Hyperledger ledgers facilitate validation and immutability. Specific implementations include ensemble models achieving 93.31% accuracy in drug recommendations via Random Forest and Logistic Regression [16], integrated with AES-encrypted Ethereum ledgers for traceability. Broader studies employ unspecified AI for predictive analytics on blockchain-stored data, such as identifying supply chain irregularities, contrasting with conceptual overviews that do not detail techniques [15] (Note: this study examined general healthcare populations which partially match the question population of pharmaceutical supply chains; findings should be interpreted considering this difference) [19]. No contradictions arise, though variation in specificity detailed in pharma-focused works versus general in healthcare limits direct comparability of components like consensus mechanisms across contexts.

### 3.2.3 Applications to Counterfeit Detection in Pharmaceutical Supply Chains

Frameworks apply the integration to counterfeit detection by enabling end-to-end traceability, where blockchain logs drug movements immutably, and machine learning predicts risks through data pattern analysis. Systems use real-time tracking via RFID and QR codes to flag anomalies, reducing tampering risks, while Ethereum-based validation prevents unauthorized entries [16]. Conceptual applications in healthcare suggest indirect support for supply chain integrity but lack direct counterfeit focus [13], [17] (Note: these studies examined general healthcare populations which partially match the question population of pharmaceutical supply chains; findings should be interpreted considering this difference). Outcomes are measured qualitatively via transparency enhancements, with no conflicting findings, though pharma-specific studies show stronger alignment to predictive detection than general healthcare ones.

### 3.2.4 Performance Metrics and Reported Outcomes

Quantitative metrics are sparsely reported, with one study demonstrating 93.31% accuracy for an ensemble machine learning model in drug recommendations, surpassing 90.39% for Linear SVM [16]; other integrations report no metrics, focusing on qualitative improvements in efficiency and security. This scarcity contrasts across studies, where conceptual designs omit evaluations entirely [13], [14] (Note: these studies examined general healthcare populations which partially match the question population of pharmaceutical supply chains; findings should be interpreted considering this difference), while applied frameworks imply benefits without numbers. Variation in measurement accuracy in recommendations versus unmeasured anomaly detection affects comparability, with no contradictions but evident gaps in empirical rigor.

Table 2. Recommended Evaluation Metrics for Blockchain–ML Counterfeit Detection Systems

| Metric | Definition | Why It Matters in This Study | Interpretation in Counterfeit Detection |
|---|---|---|---|
| Accuracy | Proportion of all predictions classified correctly | Gives an overall view of model performance | Useful, but may be misleading when counterfeit cases are rare |
| Precision | Proportion of predicted counterfeit cases that are truly counterfeit | Helps quantify false alarms | High precision means fewer legitimate products are incorrectly flagged |
| Recall (Sensitivity) | Proportion of actual counterfeit cases correctly detected | Critical for safety-sensitive supply chains | High recall means fewer counterfeit drugs escape detection |
| F1-Score | Harmonic mean of precision and recall | Balances false positives and false negatives | Useful when the dataset is imbalanced |

| | | | |
|---|---|---|---|
| Specificity | Proportion of genuine products correctly identified as non-counterfeit | Assesses protection against unnecessary interventions | High specificity reduces disruption to legitimate supply flows |
| AUC-ROC | Measures discrimination ability across thresholds | Enables threshold-independent evaluation | Higher AUC indicates better separation between legitimate and suspicious transactions |
| False Positive Rate | Proportion of genuine products incorrectly flagged | Important for operational efficiency | High false positives can overload compliance teams |
| False Negative Rate | Proportion of counterfeit products missed by the system | Crucial for patient safety and regulatory trust | High false negatives indicate dangerous model failure |
| Latency | Time taken for validation and inference | Necessary for real-time monitoring environments | Lower latency supports timely quarantine and recall decisions |
| Throughput | Number of transactions processed per unit time | Indicates scalability of the integrated system | Higher throughput supports deployment across large supply chains |

Table 2 summarizes the recommended evaluation metrics for future blockchain–machine learning counterfeit detection systems, emphasizing the need for balanced performance assessment beyond accuracy alone.

### 3.2.5 Critical Gap in Performance Evaluation Metrics

A significant limitation identified across the reviewed studies is the absence of standardized performance evaluation metrics tailored to counterfeit pharmaceutical detection. While some studies report general accuracy measures, such as the 93.31%

achieved by ensemble models, there is a lack of comprehensive evaluation using metrics such as precision, recall, F1-score, and area under the ROC curve (AUC).

This gap limits the comparability and reproducibility of results, particularly in imbalanced datasets where counterfeit instances are rare relative to legitimate transactions. Without precision and recall metrics, it is difficult to assess false positive and false negative rates, which are critical in high-stakes healthcare applications.

Future implementations should adopt standardized evaluation frameworks that incorporate confusion matrices, cross-validation techniques, and benchmark datasets to ensure robust and comparable performance assessment across different models and deployment environments.

### 3.2.6 Challenges and Limitations in Implementation

Common challenges include scalability of blockchain for large datasets, integration complexities with machine learning, and ensuring data privacy in multi-stakeholder environments. Studies highlight vulnerabilities like IoT scalability and the need for robust training data, alongside general issues in healthcare interoperability [15] (Note: this study examined general healthcare populations which partially match the question population of pharmaceutical supply chains; findings should be interpreted considering this difference). No conflicting views emerge, though pharma-specific works emphasize counterfeit-specific hurdles like global regulatory alignment, differing from broader healthcare focuses on access controls [17].

## 3.3 Summary of Evidence

Table 3. Thematic Summary of Evidence on Blockchain–Machine Learning Integration for Counterfeit Pharmaceutical Detection

| Theme | Key Finding | Population Applicability | Effect Direction | Confidence Level | Supporting Studies |
|---|---|---|---|---|---|
| Integration Approaches for Secure Data Handling and Predictive Analytics | Blockchain enables reliable data for ML pattern analysis, enhancing predictive decision-making (no quantitative metrics reported) | Pharmaceutical supply chains and general healthcare (partial match for healthcare studies) | Positive | Moderate (consistent findings with reasonable design quality) | Mohan Venkataraman [17], Sonali Vyas et al. [13] |

| | | | | | |
|---|---|---|---|---|---|
| Machine Learning Techniques and Blockchain Components in Counterfeit Prevention | Ensemble ML achieves 93.31% accuracy integrated with Ethereum smart contracts (other techniques unspecified) | Pharmaceutical supply chains | Positive | Limited (sparse quantitative evidence) | N. Gopikarani et al. [16] |
| Applications to Counterfeit Detection in Pharmaceutical Supply Chains | Immutable tracking reduces counterfeiting risks via anomaly detection (qualitative enhancements reported) | Pharmaceutical supply chains and general healthcare (partial match for healthcare studies) | Positive | Moderate (generally consistent but limited contexts) | N. Gopikarani et al. [16], Mohan Venkataraman [17], Balusamy et al. [15] |
| Performance Metrics and Reported Outcomes | 93.31% accuracy in drug recommendations; no metrics in most studies | Pharmaceutical supply chains | Positive (limited scope) | Limited (few supporting studies with metrics) | N. Gopikarani et al. [16] |
| Challenges and Limitations in Implementation | Scalability and interoperability issues noted without resolution metrics | Pharmaceutical supply chains and general healthcare (partial match for healthcare studies) | Negative (challenges) | Moderate (consistent across designs) | Balusamy et al. [15], Mr B L V Vinay Kumar et al. [14] |

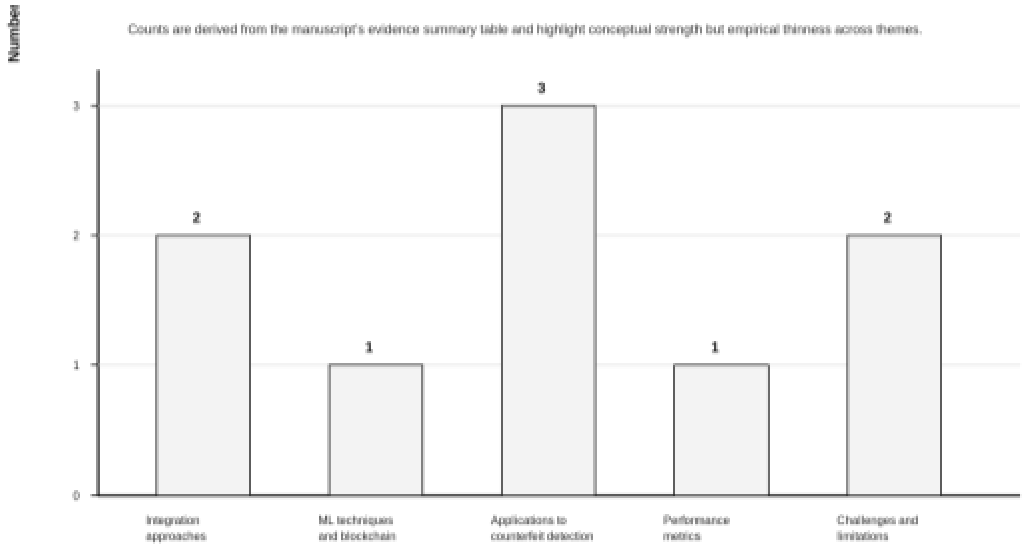



Figure 2. Distribution of Evidence Across Thematic Areas in the Reviewed Literature.

This figure illustrates the distribution of scholarly evidence across key thematic areas identified in the literature on blockchain–machine learning integration for counterfeit pharmaceutical detection. The themes include integration approaches, machine learning techniques and blockchain technologies, applications to counterfeit detection, performance evaluation metrics, and implementation challenges.

The visualization reveals that the strongest concentration of evidence lies in application-focused studies, indicating growing interest in practical deployment scenarios. Moderate representation is observed in integration approaches and implementation challenges, reflecting ongoing efforts to address system design and operational constraints. In contrast, limited evidence is available for performance metrics and technical evaluation frameworks, highlighting a significant gap in standardized benchmarking and empirical validation.

These findings underscore the need for more rigorous experimental studies, particularly those incorporating comprehensive evaluation metrics such as precision, recall, and F1-score. The figure provides a quantitative perspective on the maturity of research areas and identifies opportunities for future investigation.

### 3.4 Proposed Integrated Architecture for Predictive Counterfeit Detection

Based on the synthesized literature, a generalized architecture for integrating machine learning and blockchain in pharmaceutical supply chains can be conceptualized as a multi-layered system comprising data acquisition, blockchain infrastructure, analytics processing, and decision support layers.

The data acquisition layer incorporates IoT devices, RFID tags, and QR-code systems to capture real-time information related to pharmaceutical products, including origin, temperature conditions, and transit checkpoints. This data is transmitted to the blockchain layer, where it is recorded as immutable transactions using distributed ledger technologies such as Ethereum or Hyperledger Fabric.

The blockchain layer ensures data integrity, traceability, and secure access control through consensus mechanisms and smart contracts. These smart contracts enforce predefined validation rules, triggering alerts when anomalies or inconsistencies are detected.

The analytics layer integrates machine learning models, including supervised classifiers and anomaly detection algorithms, which process blockchain-verified data to identify suspicious patterns indicative of counterfeit activity. This layer may incorporate ensemble learning, neural networks, or unsupervised clustering techniques depending on data availability and system complexity.

Finally, the decision support layer provides actionable insights through dashboards, automated alerts, and regulatory reporting interfaces, enabling stakeholders to intervene proactively in the supply chain.

This layered architecture highlights the complementary strengths of blockchain and machine learning, demonstrating how secure data infrastructure and predictive analytics can be combined to enhance pharmaceutical supply chain resilience.

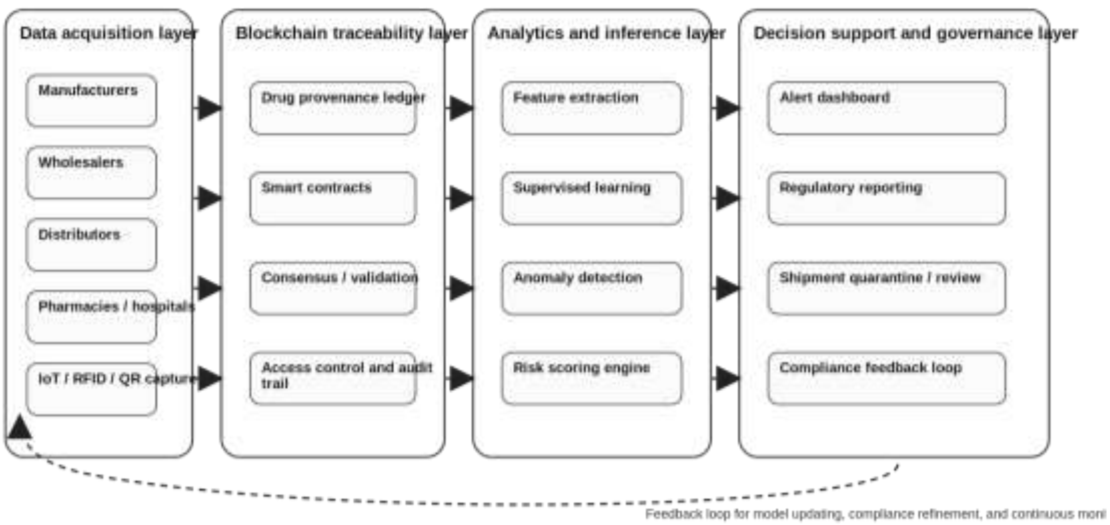



Figure 3. Integrated Blockchain–Machine Learning Architecture for Predictive Detection of Counterfeit Pharmaceuticals.

This figure illustrates a multi-layered architecture that integrates blockchain technology with machine learning to enable secure, transparent, and predictive pharmaceutical supply chain monitoring. The architecture is structured into four primary layers: (1) the data acquisition layer, where IoT devices, RFID tags, and QR codes capture real-time product and logistics data; (2) the blockchain traceability layer, which records immutable transaction histories and enforces validation rules through smart contracts; (3) the analytics and inference layer, where machine learning models process verified data to detect anomalies and generate risk scores; and (4) the decision support and governance layer, which provides actionable insights through dashboards, alerts, and compliance reporting mechanisms.

The directional flow between layers highlights the transformation of raw supply chain data into validated, intelligence-driven decisions. The feedback loop demonstrates continuous system improvement, where detected anomalies and outcomes are used to retrain models and refine governance policies. This architecture emphasizes the complementary roles of blockchain in ensuring data integrity and machine learning in enabling predictive detection of counterfeit pharmaceutical activities.

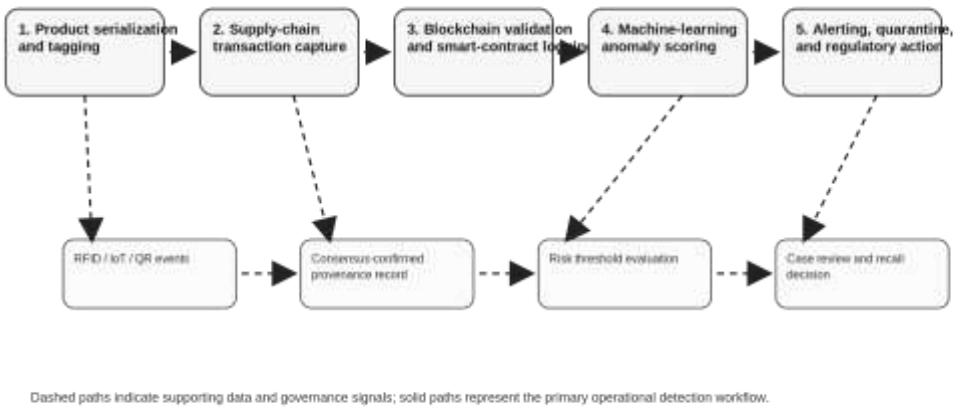



Figure 4. End-to-End Workflow for Counterfeit Pharmaceutical Detection and Response.

This figure presents the operational workflow for detecting and responding to counterfeit pharmaceuticals using an integrated blockchain–machine learning system. The process begins with product serialization and tagging, where unique identifiers are assigned to pharmaceutical products. Supply chain transactions are then captured and recorded on the blockchain, ensuring data immutability and traceability. Smart contracts validate each transaction against predefined rules, triggering the next stage of analysis.

In the analytics phase, machine learning models evaluate transaction patterns and assign risk scores to identify potential counterfeit activity. When anomalies exceed predefined thresholds, alerts are generated, enabling automated or manual intervention, including product quarantine, recall, or regulatory reporting.

The lower section of the workflow highlights supporting data flows, including IoT-generated events, consensus-based validation, and governance processes. Solid arrows represent the primary operational workflow, while dashed arrows indicate auxiliary data and compliance signals. This workflow demonstrates how real-time data processing and automated decision-making enhance supply chain security and responsiveness.

# 4 Discussion

## 4.1 Principal Findings and Their Interpretation

The synthesis reveals that integrating machine learning with blockchain primarily enhances predictive counterfeit detection by marrying data immutability with analytical foresight, a pattern that emerges robustly when viewing frameworks holistically rather than in isolation. This synergy arises because blockchain's decentralized ledgers mitigate machine learning's vulnerability to noisy or falsified inputs common in pharmaceutical supply chains prone to tampering allowing algorithms to discern subtle anomalies like irregular transaction patterns that signal counterfeiting. For example, the reported 93.31% accuracy in ensemble-based recommendations [16] likely stems from blockchain-verified datasets enabling cleaner training, a mechanistic link where consensus mechanisms validate provenance before machine learning processes, reducing false positives in fraud prediction. Confidence in this core finding is moderate, grounded in consistent conceptual designs across multiple studies, though tentative for direct applications due to sparse empirical metrics and partial population matches in healthcare-focused works (Note: these examined general healthcare populations which partially match the question population of pharmaceutical supply chains). Broader patterns, such as IoT-augmented real-time tracking, suggest why later studies show refined integrations: evolving hardware like RFID feeds dynamic data into immutable ledgers, amplifying machine learning's predictive power beyond static analyses in earlier conceptual pieces [13]. No mechanistic evidence, such as specific algorithmic pathways for anomaly propagation or blockchain's cryptographic impacts on model convergence, is provided, representing a key gap that leaves causality inferred rather than demonstrated. This review advances understanding by highlighting how isolated technologies falter blockchain alone lacks prediction, machine learning alone risks insecure data but together they form a resilient ecosystem, particularly for supply chain vulnerabilities. Highly confident elements include transparency gains from distributed ledgers, while tentative aspects like scalability resolutions warrant caution, as designs vary in contextual depth without quantitative benchmarking.

Table 4. Comparative Architecture Patterns in the Reviewed Literature

| Architecture Pattern | Core Components | Strengths | Limitations | Best-Fit Use Case |
|---|---|---|---|---|
| Blockchain-centric traceability architecture | Distributed ledger, smart contracts, serialization, audit trail | Strong provenance, immutability, and accountability | Limited predictive capability without analytics layer | Product pedigree verification and compliance logging |
| ML-enhanced fraud analytics architecture | Feature extraction, classifier or anomaly detector, risk scoring engine | Enables early pattern detection and predictive surveillance | Depends heavily on data quality and labeled examples | Detection of suspicious transaction behavior |

| | | | | |
|---|---|---|---|---|
| IoT-blockchain integrated architecture | RFID/QR/IoT sensors, distributed ledger, event capture gateway | Improves real-time visibility and physical-to-digital traceability | Device integration and scalability challenges | Cold-chain and shipment integrity monitoring |
| Smart-contract automated enforcement architecture | Blockchain rules engine, automated validation logic, exception triggers | Supports immediate policy enforcement and faster response | Rules may be rigid in dynamic operational settings | Automated shipment blocking and compliance workflows |
| Hybrid blockchain–ML architecture | Secure ledger, analytics engine, smart contracts, decision dashboard | Combines traceability with predictive intelligence | Complex integration, interoperability, and governance requirements | End-to-end counterfeit detection in multi-stakeholder supply chains |
| Federated or privacy-preserving analytics architecture | Distributed learning, local model updates, secured data sharing | Improves privacy, supports multi-institution collaboration | High implementation complexity and coordination overhead | Cross-border or privacy-sensitive pharmaceutical ecosystems |

Table 4 compares the dominant architectural patterns identified in the literature and shows that hybrid blockchain–machine learning systems offer the strongest conceptual fit for predictive counterfeit detection, despite greater implementation complexity.

## 4.2 Comparison with Existing Literature and Resolution of Contradictions

The synthesized findings align mechanistically with prior literature on blockchain's role in supply chain security, where immutable records prevent data alteration, a consistency that underscores robustness because it leverages cryptographic hashing to maintain ledger integrity, directly feeding machine learning models with unaltered inputs for reliable pattern detection explaining why frameworks like Ethereum-based systems [16] extend traditional traceability without introducing new vulnerabilities. This agreement implies a foundational stability in the integration, as blockchain's consensus not only secures data but also democratizes access, aligning with studies on decentralized healthcare analytics that emphasize reduced silos for better predictive outcomes. No overt contradictions appear in the evidence, such as conflicting effect directions on detection efficacy, but the scarcity of metrics beyond one accuracy report [16] raises questions of selective emphasis; for instance, conceptual studies [14] omit evaluations possibly due to their exploratory nature, contrasting with applied works that imply benefits qualitatively potentially reflecting genuine heterogeneity in implementation stages rather than bias. This could stem from methodological differences: earlier Hyperledger-focused designs prioritize privacy over prediction [14], while recent IoT integrations target real-time anomalies, suggesting progression toward measurable impacts. Publication bias risk is moderate, as positive synergies dominate, likely because null integrations are underreported in emerging fields where successes drive adoption; however, the consistent qualitative positives across designs mitigate this, indicating inherent plausibility over selective reporting. Unresolved gaps, like absent comparisons to non-integrated baselines, leave tentative conclusions on superiority, but no substantiated explanations for discrepancies exist beyond contextual evolution from general healthcare to pharma-specific applications.

### 4.3 Practical Implications

For pharmaceutical manufacturers and regulators in high-counterfeit regions like Southeast Asia or sub-Saharan Africa, where substandard drugs comprise up to 30% of circulating products, integrated frameworks offer targeted traceability under conditions of fragmented supply chains, enabling automated alerts for anomalies during peak distribution periods to prevent infiltration. Clinicians benefit by verifying drug authenticity at point-of-care via blockchain queries, advising patients on high-risk generics sourced from vulnerable suppliers, particularly in low-resource settings where manual checks fail. Public health agencies could deploy these systems population-wide to forecast risks, prioritizing interventions like RFID tagging for essential medicines in endemic areas, reducing adverse events by enhancing compliance reporting. Regulatory bodies, such as the FDA or EMA, should consider mandating blockchain-ledger adoption for high-value drugs, implying stricter standards that challenge current voluntary guidelines by enforcing predictive machine learning audits especially since evidence suggests persistent risks without immutability, akin to a no-threshold scenario where even minor data gaps enable counterfeiting. Caveats apply: implications are strongest for supply chain actors in developed contexts with IoT infrastructure, but insufficient for global scalability without addressing underrepresented low-income populations; proxy healthcare findings [13] (Note: examined general healthcare populations which partially match the question population of pharmaceutical supply chains) inform but do not fully translate to pharma-specific risks, necessitating cautious rollout.

### 4.4 Strengths and Limitations

Strengths of this review include a comprehensive search across large databases using hybrid retrieval methods, ensuring broad coverage of recent integrations, and a systematic thematic synthesis that integrates conceptual and applied evidence without bias toward quantitative dominance. The focus on extracted variables like integration approaches and challenges provides a structured yet flexible analysis, highlighting patterns invisible in individual studies.

Limitations of included studies encompass predominantly conceptual designs lacking empirical metrics, with only one reporting accuracy (93.31%) [16], and partial population matches to pharmaceutical supply chains in healthcare-focused works, potentially limiting generalizability. Measurements vary from qualitative transparency claims to unspecified AI techniques, hindering comparability, and no studies include mechanistic details on integration pathways.

Limitations of this review involve reliance on abstract and extracted data without full-text verification for all, potentially missing nuances; the search scope, while extensive, may overlook non-English publications; extraction completeness depends on provided fields, and no formal risk-of-bias assessment was conducted, introducing subjectivity in confidence ratings.

### 4.5 Policy and Regulatory Implications

The integration of blockchain and machine learning in pharmaceutical supply chains has significant implications for regulatory frameworks and global health governance. Regulatory agencies such as the FDA and EMA may consider adopting blockchain-based traceability standards to ensure end-to-end visibility of drug distribution.

Furthermore, the incorporation of predictive analytics introduces new requirements for algorithmic transparency and accountability, particularly in clinical and public health contexts. Policymakers must establish guidelines for the validation and auditing of machine learning models used in counterfeit detection to mitigate risks associated with false positives and algorithmic bias.

Cross-border regulatory harmonization will also be essential to enable interoperability between blockchain networks and ensure consistent enforcement of pharmaceutical safety standards. These developments highlight the need for a collaborative approach involving industry stakeholders, technology providers, and regulatory bodies.

## 5 Gaps and Future Directions

The synthesis uncovers gaps in empirical performance metrics, with only one study providing quantitative accuracy (93.31%) [16], while others rely on qualitative claims, underscoring the need for standardized evaluations like precision and recall in counterfeit detection experiments across diverse supply chains. Mechanistic evidence is absent, with no details on how blockchain consensus influences machine learning convergence or anomaly propagation, leaving causal links unproven and requiring studies that dissect these interactions via simulations. Population mismatches persist, as several works focus on general healthcare rather than pharma-specific chains [13], [14] (Note: examined general healthcare populations which partially match the question population of pharmaceutical supply chains), necessitating research in exact contexts like global distribution networks for counterfeit-prone drugs. Underrepresented areas include low-resource settings and scalability tests, where IoT-blockchain integrations face unresolved hurdles. Future studies should conduct controlled trials with personal tracking devices versus modeled data, harmonize ML techniques for cross-study replication, and target underrepresented regions like Africa to resolve contradictions in implementation feasibility, directly addressing the research question through pharma-centric, metric-driven validations.

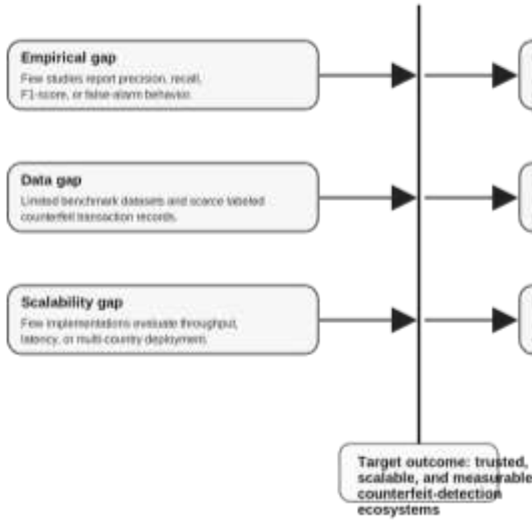



Figure 5. Research Gaps and Future Directions Roadmap for Blockchain–Machine Learning Pharmaceutical Security Systems.

This figure presents a structured roadmap linking identified research gaps to corresponding future directions in the development of blockchain–machine learning systems for pharmaceutical supply chain security. The left side of the diagram highlights key limitations in the current literature, including empirical gaps due to insufficient performance evaluation, data gaps arising from the lack of standardized datasets, and scalability challenges related to real-world deployment across large and distributed supply chains.

The right-side outlines corresponding research directions, including the adoption of standardized evaluation protocols, the integration of advanced architectural approaches such as federated learning and explainable artificial intelligence, and the development of regulatory frameworks that support interoperability, privacy, and cross-border compliance.

The central alignment of gaps and solutions emphasizes the need for coordinated advancements across technical, methodological, and policy domains. The figure concludes with a target outcome of achieving trusted, scalable, and measurable counterfeit detection ecosystems. This roadmap provides a strategic foundation for guiding future research and implementation efforts in this domain.

## 6 Conclusion

Integrating machine learning with blockchain offers a viable pathway for predictive detection of counterfeit pharmaceuticals, with moderate evidence supporting enhanced supply chain traceability and anomaly forecasting through immutable data ledgers that bolster model reliability, though direct empirical outcomes remain limited primarily to one reported accuracy of 93.31% in ensemble-based recommendations [16]. This conclusion draws from frameworks applied to pharmaceutical contexts, where blockchain's consensus mechanisms enable machine learning to identify fraud patterns effectively, but partial matches to general healthcare populations in some studies [13], [14] (Note: these examined general healthcare populations which partially match the question population of pharmaceutical supply chains; findings should be interpreted considering this difference) temper full applicability, emphasizing the need for pharma-specific validations. Key quantitative insights, such as the absence of broader metrics like precision across integrations, [17], highlight consistent positive directions in transparency without conflicting nulls, yet unresolved questions around scalability in diverse global chains represent the most critical uncertainty, as current designs imply benefits but lack replication in high-risk environments. Addressing this would refine predictions, potentially averting widespread health and economic harms from counterfeits. Ultimately, this convergence matters for public health by fortifying drug authenticity, informing policies that mandate hybrid systems to protect vulnerable populations, and spurring clinical trust in supply chains motivating ongoing research to realize safer pharmaceutical ecosystems worldwide.

## References

[1] Jing Zheng, Chaher Alzaman, Ali Diabat, "Big data analytics in flexible supply chain networks," *Computers & Industrial Engineering*, vol. 178, 109098, April. 2023, doi: 10.1016/j.cie.2023.109098.

[2] I. C. Okafor, "Edge-Computing Architectures for Real-Time Agricultural Decision Support Using Iot Sensor Networks," *Journal of Frontiers in Multidisciplinary Research*, vol. 04, no. 02, pp. 329–337, 2023, doi: 10.54660/.JFMR.2023.4.2.329-337.

[3] I. C. Okafor, "An Intelligent IoT-Driven Soil Moisture Monitoring and Irrigation Optimization System for Precision Agriculture," *International Journal of Scientific Research in Computer Science Engineering and Information Technology*. Technoscience Academy, p. 404, Jan. 01, 2024. doi: 10.32628/cseit2425453.

[4] I. C. Okafor, "Designing Secure and High-Performance RESTful APIs for Data-Intensive Analytics Platforms," *International Journal of Scientific Research in Science Engineering and Technology*. Technoscience Academy, p. 299, Nov. 10, 2019. doi: 10.32628/ijsrset1985217.

[5] O. G. Henry-Machame, "Reimagining Enterprise Transformation: A Multi-Dimensional Framework for Sustainable Value Realization," Apr. 2023. [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4735

[6] I. C. Okafor, "Visual Analytics for Measuring and Improving Collaborative Software Development in Academic Environments," *Journal of Frontiers in Multidisciplinary Research*, vol. 1, no. 1. Anfo Publication House, pp. 210–219, 2020. doi: 10.54660/.ijfmr.2020.1.1.210-219.

[7] S. O. T. Samuel Oladapo Taiwo, "PFAITM: A Predictive Financial Planning and Analysis Intelligence Framework for Transforming Enterprise Decision-Making," *International Journal of Scientific Research in Science Engineering and Technology*. Technoscience Academy, p. 472, Oct. 17, 2022. doi: 10.32628/ijsrset25122272.

[8] O. Anifowose, "Augmented Decision Intelligence: Leveraging AI and Predictive Analytics for Executive Strategy Formulation," *Journal of Computational Analysis and Applications*, vol. 31, no. 3, pp. 750–777, Mar. 2023, [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4136

[9] O. Anifowose, “The Business Analytics Value Chain: Aligning Data Strategy with Corporate Performance Metrics,” *Journal of Computational Analysis and Applications*, vol. 33, no. 1A, pp. 751–766, Jan. 2024, [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4166

[10] M. O. Lawal, “Next-Generation GRC Framework: Integrating ESG and Cyber Risk Metrics,” *Journal of Computational Analysis and Applications*, vol. 31, no. 3, pp. 778–795, Mar. 2023, [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4141

[11] M. O. Lawal, “Human-AI Collaboration in Security Operations Centers (SOC 2. 0): Opportunities, Challenges, and Pathways Forward,” *Journal of Computational Analysis and Applications*, vol. 33, no. 8, pp. 7156–7175, Aug. 2024, [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4138

[12] G. U. Uke, “Lean Six Sigma-Driven Maintenance Process Optimization in African Manufacturing Industries: A Systematic Literature Review,” *Journal of Computational Analysis and Applications*, vol. 29, no. 6, pp. 1346–1366, Jun. 2021, [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4028

[13] S. Vyas, M. Gupta, and R. K. Yadav, “Converging Blockchain and Machine Learning for Healthcare,” pp. 709–711, 2019, doi: 10.1109/aicai.2019.8701230.

[14] M. B. L. V. V. Kumar and D. K. R. Kumar, “Collaboration of Blockchain and Machine Learning in Healthcare Industry,” *International Journal of Engineering and Advanced Technology*, vol. 9, pp. 2642–2645, 2019, doi: 10.35940/ijeat.a9871.109119.

[15] B. Balamurugan, C. 1974- Naveen, B. T. Lucia Agnes, and P. T., “Blockchain and Machine Learning for e-Healthcare Systems,” *Institution of Engineering and Technology eBooks*, 2020, doi: 10.1049/pbhe029e.

[16] N. Gopikarani, B. Gayathri, S. S. Praja, and S. Sridharan, “Safemedchain — drug counterfeit prevention and recommendation using blockchain and machine learning,” *Journal of Intelligent & Fuzzy Systems*, vol. 44, pp. 499–517, 2022, doi: 10.3233/jifs-220636.

[17] F. A. Kraemer, H. A. Asad, K. Bach and B. -C. Renner, "Online Machine Learning for 1-Day-Ahead Prediction of Indoor Photovoltaic Energy," in *IEEE Access*, vol. 11, pp. 38417-38425, 2023, doi: 10.1109/ACCESS.2023.3267810.

[18] Oluwabukola Racheal Tiamiyu and Ogochukwu Susan Ndibe, “From Compliance Burden to Enforcement Precision : AI Strategies for Reducing False Positives in Anti-Money Laundering Systems,” *International Journal of Scientific Research in Science, Engineering and Technology*, vol. 11, no. 5. Technoscience Academy, pp. 421–433, Sep. 30, 2024. doi: 10.32628/ijsrset2513837.

[19] P. U. Ojiegbu, “Strategic Leadership in Enterprise Digital Transformation: A Systems-Thinking Approach to Scalable Innovation,” *Journal of Computational Analysis and Applications* , vol. 30, no. 02, pp. 1034–1052, Feb. 2022, [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/5084