SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

SECURE SUPPLY CHAIN MANAGEMENT USING BLOCKCHAIN & ANOMALY DETECTION SYSTEM USING PYTHON, AI & ML

Dr. Uppe Nanaji [1], Dr. C P V N J Mohan Rao[2], K. Vara Prasad[3]
[1,2]Professor in CSE Dept, Avanthi Institute of Engg & Technology, Anakapalle
[3]Asst Prof in CSE Dept, Avanthi Institute of Engg & Technology, Anakapalle3

ABSTRACT

Modern supply chains are complex networks susceptible to numerous vulnerabilities, including fraud, counterfeiting, inefficiencies, and lack of transparency. This paper proposes an integrated system leveraging blockchain technology for enhanced security and traceability, coupled with an Artificial Intelligence (AI) and Machine Learning (ML) based anomaly detection system implemented in Python. Blockchain provides an immutable and transparent ledger for recording transactions and tracking goods, thereby fostering trust among participants. The AI/ML anomaly detection system analyzes data from the supply chain (including blockchain records and sensor data) to identify unusual patterns, potential disruptions, or fraudulent activities in real-time. This synergistic approach aims to create a more resilient, secure, and efficient supply chain ecosystem. The paper details the architecture of this integrated system, discusses the roles of blockchain and AI/ML components, explores conceptual implementation aspects, and highlights the potential benefits and challenges.

KEYWORDS: *Supply Chain Management (SCM), Blockchain Technology, Artificial Intelligence (AI), Machine Learning (ML), Anomaly Detection, Python, Cyber security, Transparency, Traceability, Smart Contracts.*

1. INTRODUCTION

Supply Chain Management (SCM) is the backbone of global commerce, encompassing the planning, execution, and control of all activities involved in sourcing, procurement, conversion, and logistics management. However, traditional SCM systems often suffer from opacity, fragmentation, and susceptibility to various risks. These challenges can lead to significant financial losses, reputational damage, and compromised consumer safety.

1.1 Challenges in Traditional Supply Chain Management Traditional supply chains are characterized by:

- **Lack of Transparency:** Difficulty in tracking products from origin to consumer, leading to information silos.
- **Inefficiency:** Manual processes, redundant paperwork, and poor communication contribute to delays and increased costs.
- **Security Vulnerabilities:** Susceptibility to theft, counterfeiting, product tampering, and data breaches.
- **Data Integrity Issues:** Centralized databases are prone to manipulation and single points of failure.
- **Complex Dispute Resolution:** Lack of a single source of truth complicates the resolution of disputes among stakeholders.

1.2 Potential of Blockchain in SCM Blockchain technology, a distributed and immutable ledger, offers a transformative solution to many SCM challenges. Its core features include:

- **Decentralization:** Data is distributed across a network of computers, eliminating single points of failure.
- **Immutability:** Once a transaction is recorded on the blockchain, it cannot be altered or deleted.
- **Transparency:** Authorized participants can view relevant transaction history, fostering trust.
- **Traceability:** Products and components can be tracked at every stage of the supply chain.
- **Smart Contracts:** Self-executing contracts with predefined rules can automate processes like payments and compliance checks.

1.3 Role of AI/ML in Anomaly Detection for SCM While blockchain enhances data integrity and transparency, Artificial Intelligence (AI) and Machine Learning (ML) can provide intelligent insights by analyzing the vast amounts of data generated within the supply chain. Anomaly detection, a key application of AI/ML, involves identifying data points or patterns that deviate significantly from the norm. In SCM, this can help in:

- Proactively identifying potential disruptions (e.g., unexpected delays, equipment failures).
- Detecting fraudulent activities (e.g., counterfeit products, unauthorized transactions).
- Monitoring compliance with regulations and quality standards.
- Optimizing logistics and inventory management by identifying inefficiencies.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

1.4 Thesis Statement and Paper Structure This paper posits that integrating blockchain technology for secure and transparent data management with an AI/ML-powered anomaly detection system (implemented using Python) can create a significantly more robust, resilient, and efficient supply chain. The proposed system aims to provide end-to-end visibility, ensure data integrity, automate key processes through smart contracts, and proactively identify and mitigate risks through intelligent data analysis.
The remainder of this paper is structured as follows: Section 2 provides a literature review. Section 3 details the proposed integrated system architecture. Section 4 discusses conceptual implementation aspects. Section 5 outlines the benefits of the system. Section 6 addresses challenges and future directions. Section 7 concludes the paper.

2. LITERATURE REVIEW

This section reviews existing research on the application of blockchain in SCM and the use of AI/ML for anomaly detection in this domain, identifying the gaps that an integrated approach can address.

2.1 Blockchain in Supply Chain Management: Existing Work and Benefits The application of blockchain in SCM has gained considerable attention. Researchers like Kshetri (2018) highlighted blockchain's potential to enhance transparency and traceability, particularly in combating counterfeit goods. Saberi et al. (2019) proposed a conceptual framework for blockchain-based SCM, emphasizing improved efficiency and trust. Studies by Tijan et al. (2019) explored blockchain's role in maritime logistics, demonstrating benefits in documentation and process streamlining. Key benefits cited in the literature include:

- **Enhanced Traceability:** Tracking products from source to consumer (e.g., Walmart's use of Hyperledger Fabric for food traceability).
- **Improved Security:** Reducing fraud and counterfeiting through immutable records.
- **Increased Efficiency:** Automating processes via smart contracts and reducing paperwork.
- **Greater Transparency:** Providing a shared, trusted view of information to all stakeholders.

2.2 AI and ML for Anomaly Detection in Supply Chains: Techniques and Applications AI and ML techniques have been widely applied for anomaly detection across various domains, including SCM. Chandola et al. (2009) provide a comprehensive survey of anomaly detection techniques, categorizing them into statistical, clustering-based, and classification-based methods. In SCM, AI/ML has been used for:

- **Demand Forecasting Anomalies:** Identifying unusual spikes or drops in demand (Fildes et al., 2008).
- **Fraud Detection:** Detecting fraudulent orders or supplier activities (Ngai et al., 2011).
- **Quality Control:** Identifying defective products based on sensor data or production parameters.
- **Logistics Optimization:** Detecting inefficiencies or disruptions in transportation routes. Common ML algorithms include Isolation Forest, One-Class SVM, Autoencoders (for unsupervised detection), and Random Forest, Gradient Boosting (for supervised detection when labeled anomaly data is available). Time-series models like ARIMA and LSTMs are also crucial for detecting anomalies in sequential SCM data.

2.3 Gaps and Opportunities for an Integrated Approach While blockchain provides a secure data foundation and AI/ML offers intelligent analysis, much of the existing research treats these technologies in isolation for SCM.

- Blockchain systems generate vast amounts of trusted data, but often lack sophisticated analytical capabilities to derive actionable insights or predict issues proactively.
- AI/ML systems can detect anomalies, but their effectiveness is dependent on the quality and integrity of the input data. Centralized or untrusted data sources can compromise AI/ML models.

An integrated system, where AI/ML algorithms operate on trusted, immutable data from a blockchain, presents a significant opportunity. The blockchain can ensure the provenance and integrity of data used for training and running anomaly detection models. In turn, AI/ML can enhance the value of the blockchain by identifying critical events or risks that might require attention or even trigger smart contract actions. This paper focuses on architecting such an integrated system.

3. PROPOSED INTEGRATED SYSTEM ARCHITECTURE

The proposed system integrates a Blockchain Layer for secure data management with an AI/ML Anomaly Detection Layer for intelligent risk identification which is shown in Figure 1.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

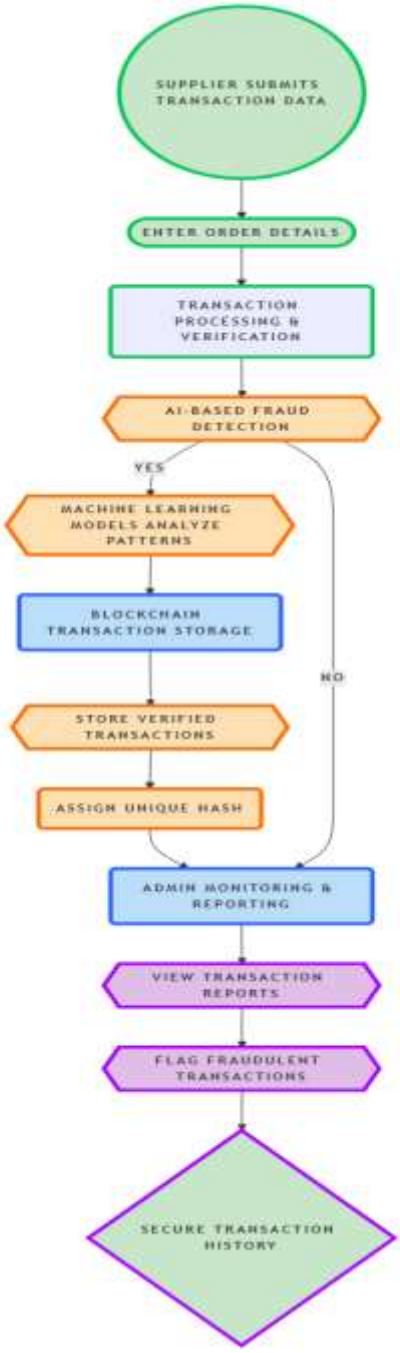

Figure 1 illustrates the flow of data within the Secure Supply Chain Management System

3.1 Blockchain Layer for Secure SCM

This layer forms the trusted data backbone of the supply chain.

- **Participants and Roles**
  - **Manufacturer:** Creates products, registers them on the blockchain.
  - **Supplier:** Provides raw materials/components, records their origin and quality.
  - **Logistics Provider:** Manages transportation, updates shipment status and conditions (e.g., temperature for perishables via IoT integration).

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

- **Distributor/Wholesaler:** Manages inventory, records handovers.
- **Retailer:** Receives products, manages sales.
- **Consumer:** Can verify product authenticity and history.
- **Regulator/Auditor:** Can access relevant data for compliance checks (with appropriate permissions).

- **Data Model and Transactions on Blockchain:**
  - **Digital Asset Representation:** Each product or batch is represented as a unique digital asset (token) on the blockchain.
  - **Key Data Points:** Product ID, batch number, manufacturing date, origin, certifications, ownership history, shipment details (location, timestamp, carrier), environmental conditions (if applicable from IoT sensors), quality inspection results.
  - **Transactions:** Creation of asset, transfer of ownership, shipment updates, quality attestations, customs clearance. Each transaction is digitally signed and time-stamped.
- **Smart Contracts for Automation and Trust:** Smart contracts automate various SCM processes and enforce business rules:
  - **Track and Trace:** Automatically update product location and status.
  - **Quality Assurance:** Trigger alerts or hold payments if quality parameters (e.g., from IoT sensors) are not met.
  - **Automated Payments:** Release payments to suppliers upon successful delivery and verification (Delivery vs. Payment).
  - **Compliance Checks:** Verify if shipments meet regulatory requirements.
  - **Dispute Resolution:** Provide an immutable record for resolving disputes.
- **Choice of Blockchain Platform:**
  - **Hyperledger Fabric:** A permissioned blockchain framework suitable for enterprise SCM due to its modularity, scalability, support for private channels, and fine-grained access control.
  - **Ethereum:** Can be used as a permissioned (private) network or leveraging Layer 2 solutions for scalability if public network aspects are desired for certain use cases (though less common for enterprise SCM core operations). The choice depends on specific requirements regarding governance, privacy, performance, and existing infrastructure. Hyperledger Fabric is often favored for its enterprise focus.

3.2 AI/ML Anomaly Detection Layer

This layer analyzes data to identify deviations from normal behavior.

- **Data Sources and Collection**
  - **Blockchain Data:** Transaction logs, asset states, smart contract events.
  - **IoT Sensor Data:** Real-time data on temperature, humidity, shock, location (often integrated with blockchain transactions).
  - **Enterprise Resource Planning (ERP) / SCM Systems:** Order data, inventory levels, supplier performance metrics.
  - **External Data:** Weather information, traffic data, market trends. Data is collected and aggregated into a data lake or warehouse for analysis.
- **Data Preprocessing and Feature Engineering**
  - **Data Cleaning:** Handling missing values, removing noise, correcting inconsistencies.
  - **Data Transformation:** Normalization, scaling, encoding categorical variables.
  - **Feature Engineering:** Creating relevant features for anomaly detection, such as:
    - Transaction frequency/volume.
    - Deviation from planned routes/schedules.
    - Unusual changes in sensor readings.
    - Time lags between SCM stages.
    - Order patterns (e.g., unusually large orders, orders from new/unverified locations).
- **Anomaly Detection Models:** A combination of unsupervised and supervised techniques is often most effective:
  - **Unsupervised Learning (for unknown anomalies):**
    - **Clustering:** K-Means, DBSCAN to group similar transactions/events and identify outliers.
    - **Density-Based:** Local Outlier Factor (LOF).
    - **Tree-Based:** Isolation Forest, highly efficient for large datasets.
    - **Neural Networks:** Autoencoders to learn normal patterns and identify deviations by reconstruction error.
  - **Supervised Learning (if labeled historical anomaly data is available):**
    - **Classification:** Support Vector Machines (SVM), Random Forest, Gradient Boosting to classify events as normal or anomalous.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

- **Time-Series Analysis (for sequential data):**
  - ARIMA, Exponential Smoothing.
  - Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTMs) to model temporal dependencies and detect unusual sequences or deviations from forecasts.

- **Implementation using Python and relevant libraries:**
  - **Data Manipulation:** Pandas, NumPy.
  - **Machine Learning:** Scikit-learn (for most classical ML models like Isolation Forest, SVM, Random Forest), PyOD (Python Outlier Detection library).
  - **Deep Learning:** TensorFlow, Keras, PyTorch (for Autoencoders, LSTMs).
  - **Data Visualization:** Matplotlib, Seaborn (for understanding data and anomaly patterns).

3.3 Integration Framework: Blockchain and AI/ML Synergy

- **Data Flow and Interaction Points:**
  1. SCM transactions and IoT data are recorded on the Blockchain Layer.
  2. The AI/ML Anomaly Detection Layer periodically (or in real-time via event listeners) ingests data from the blockchain and other integrated SCM systems.
  3. AI/ML models process the data to detect anomalies.
  4. Detected anomalies are flagged and analyzed for severity and potential impact.
- **Alerting Mechanisms and Response Protocols:**
  1. **Alert Generation:** High-risk anomalies trigger alerts to relevant stakeholders (e.g., supply chain managers, security personnel) via dashboards, email, or SMS.
  2. **Investigation:** Human operators investigate the flagged anomalies to confirm their nature and root cause.
  3. **Automated Response (via Smart Contracts - with caution):**
     - For certain predefined and high-confidence anomalies, the AI system could potentially trigger actions via smart contracts (e.g., temporarily halting a shipment, flagging a product batch for inspection, or holding a payment). This requires robust validation and often human oversight.
  4. **Feedback Loop:** Confirmed anomalies and their resolutions are fed back into the AI/ML system to improve model accuracy and adapt to new types of anomalies. Insights can also inform updates to smart contract rules or business processes.
  5. **Reporting:** Dashboards provide visualizations of supply chain health, detected anomalies, and trends.

4. CONCEPTUAL IMPLEMENTATION DETAILS

This section provides a high-level view of how key components might be implemented.

4.1 Illustrative Smart Contract Logic (Pseudocode for Hyperledger Fabric Chaincode)

```
// Smart Contract: ProductTracking

// Structure for a Product
Product {
    ID: string
    Name: string
    Manufacturer: string
    ManufactureDate: timestamp
    CurrentOwner: string
    Status: string (e.g., "InTransit", "Delivered", "QualityCheck")
    LocationHistory: array of {Location: string, Timestamp: timestamp, Carrier: string}
    SensorReadings: array of {Temperature: float, Timestamp: timestamp} // Example for perishables
    Anomalies: array of {Type: string, Timestamp: timestamp, Details: string}
}

// Function to register a new product
function registerProduct(ID, Name, Manufacturer):
    // Check if caller is authorized (e.g., registered manufacturer)
```

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

```
    // Create new Product asset
    // Store Product on ledger
    // Emit event: ProductRegistered

// Function to transfer ownership and update status/location
function updateShipment(ProductID, NewOwner, NewStatus, CurrentLocation, Carrier,
OptionalSensorData):
    // Get Product from ledger
    // Verify caller's identity (e.g., current owner or authorized logistics provider)
    // Update Product.CurrentOwner, Product.Status
    // Add to Product.LocationHistory
    // If SensorData provided, add to Product.SensorReadings
        // (Optional: Check sensor data against predefined thresholds within smart contract)
        // If threshold breached, update Product.Status to "QualityIssue"
    // Store updated Product on ledger
    // Emit event: ShipmentUpdated

// Function to record a detected anomaly (potentially called by an authorized off-chain
service)
function flagAnomaly(ProductID, AnomalyType, AnomalyDetails):
    // Get Product from ledger
    // Verify caller (e.g., authorized AI service or admin)
    // Add to Product.Anomalies array
    // Store updated Product on ledger
    // Emit event: AnomalyFlagged
```

4.2 Python-based Anomaly Detection Workflow (Conceptual Snippets)

```
import pandas as pd
from sklearn.ensemble import IsolationForest
from sklearn.preprocessing import StandardScaler
# Assume 'blockchain_data_fetcher' is a module to get data from the blockchain
# Assume 'iot_data_fetcher' is a module to get sensor data

# 1. Data Ingestion
# raw_blockchain_data = blockchain_data_fetcher.get_transactions(last_n_hours=24)
# raw_iot_data = iot_data_fetcher.get_sensor_readings(last_n_hours=24)

# Example: Mock data for illustration
data = {
    'transaction_id': [1, 2, 3, 4, 5, 6, 7, 8, 9, 10],
    'product_id': ['P101', 'P102', 'P101', 'P103', 'P102', 'P101', 'P104', 'P105', 'P103',
'P101'],
    'quantity': [100, 150, 110, 200, 160, 5000, 90, 120, 210, 95], # Anomaly: 5000
    'value': [1000, 1500, 1100, 2000, 1600, 50000, 900, 1200, 2100, 950], # Anomaly: 50000
    'ship_time_hours': [24, 30, 26, 48, 32, 72, 20, 28, 50, 120], # Anomaly: 120
    'temperature_celsius': [4, 5, 4.5, 25, 5.5, 4, 6, 4.2, 3.8, 5] # Anomaly: 25 (if
perishable)
}
df = pd.DataFrame(data)

# 2. Feature Engineering & Preprocessing
# Example: Select numerical features for anomaly detection
features = ['quantity', 'value', 'ship_time_hours', 'temperature_celsius']
X = df[features]
```

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

```
# Scale features
scaler = StandardScaler()
X_scaled = scaler.fit_transform(X)

# 3. Anomaly Detection Model (Isolation Forest example)
# Contamination: expected proportion of outliers in the data set
model = IsolationForest(n_estimators=100, contamination='auto', random_state=42)
model.fit(X_scaled)

# Predict anomalies (-1 for outliers, 1 for inliers)
df['anomaly_score'] = model.decision_function(X_scaled)
df['is_anomaly'] = model.predict(X_scaled)

# 4. Alerting and Reporting
anomalies_df = df[df['is_anomaly'] == -1]
print("Detected Anomalies:")
print(anomalies_df)

# if not anomalies_df.empty:
#     # Send alerts (e.g., email, push notification)
#     # alert_system.send_alerts(anomalies_df)
#     # Potentially trigger investigation or smart contract interaction
#     for index, row in anomalies_df.iterrows():
#         # blockchain_connector.call_smart_contract('flagAnomaly', row['product_id'],
'UnusualActivity', row.to_json())
#         pass

# 5. Model Retraining (Periodically)
# This would involve retraining the model with new data, potentially incorporating feedback
on confirmed anomalies.
```

Disclaimer: The Python code is illustrative and simplified. A production system would require robust data pipelines, error handling, model versioning, and comprehensive testing.

5. BENEFITS OF THE INTEGRATED SYSTEM

The proposed integrated system offers numerous advantages:

- **Enhanced Security and Fraud Prevention:** Blockchain's immutability makes it extremely difficult to tamper with transaction records, reducing fraud and counterfeiting. AI/ML proactively identifies suspicious activities that might indicate security breaches or illicit actions.
- **Increased Transparency and Traceability:** All stakeholders with appropriate permissions can access a shared, real-time view of the supply chain, from raw material sourcing to final delivery. This allows for full product provenance.
- **Improved Efficiency and Reduced Operational Costs:** Smart contracts automate manual processes like paperwork, compliance checks, and payments, reducing administrative overhead and delays. Anomaly detection helps prevent costly disruptions.
- **Proactive Risk Management:** AI/ML models can predict potential issues (e.g., delays, quality degradation, equipment failure) before they escalate, allowing for timely intervention.
- **Better Compliance and Auditing:** The immutable and time-stamped record on the blockchain simplifies auditing and compliance with industry regulations and standards.
- **Increased Trust Among Supply Chain Partners:** A shared, verifiable source of truth fosters greater trust and collaboration among participants.
- **Data-Driven Decision Making:** Insights from AI/ML analysis of trusted blockchain data enable more informed strategic and operational decisions.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

- **Enhanced Consumer Confidence:** Consumers can verify the authenticity and ethical sourcing of products, leading to increased brand loyalty.

6. CHALLENGES AND FUTURE DIRECTIONS

Despite the significant potential, the implementation of such an integrated system faces several challenges and offers avenues for future research.

6.1 Technical Challenges

- **Blockchain Scalability:** Public blockchains can have limitations in transaction throughput. Permissioned blockchains like Hyperledger Fabric offer better scalability but still require careful design for high-volume supply chains.
- **Interoperability:** Integrating different blockchain systems used by various partners and connecting them with legacy SCM systems can be complex.
- **Data Privacy and Confidentiality:** While transparency is a benefit, sensitive business data on the blockchain needs robust permissioning and encryption mechanisms (e.g., private data collections in Hyperledger Fabric, zero-knowledge proofs).
- **AI/ML Model Interpretability (Explainability):** Understanding why an AI model flags a particular event as an anomaly can be challenging, especially with complex models like deep neural networks.
- **Data Quality for AI:** The adage "garbage in, garbage out" applies. While blockchain ensures data integrity once recorded, the initial data input must be accurate.
- **Dynamic Anomaly Patterns:** Anomalies evolve; AI models need continuous monitoring and retraining to remain effective.

6.2 Implementation and Adoption Hurdles

- **Cost of Implementation:** Setting up and maintaining a blockchain infrastructure and an AI/ML system can be expensive.
- **Adoption Barriers:** Convincing all supply chain partners to adopt a new technology and share data requires significant effort and clear value propositions.
- **Lack of Standardization:** Standardized data formats and protocols are needed for seamless interoperability across the supply chain.
- **Regulatory Uncertainty:** The legal and regulatory landscape for blockchain and AI is still evolving in many jurisdictions.
- **Skill Gap:** A shortage of professionals with expertise in both blockchain and AI/ML for SCM.

6.3 Ethical Considerations

- **Bias in AI Models:** If training data reflects historical biases, AI models may perpetuate or amplify these biases in anomaly detection (e.g., unfairly targeting certain suppliers or routes).
- **Data Ownership and Governance:** Clear rules are needed for data ownership, access rights, and governance of the integrated platform.

6.4 Future Directions

- **Integration with IoT:** Deeper integration with Internet of Things (IoT) devices for real-time, automated data capture (e.g., environmental sensors, GPS trackers) directly onto the blockchain.
- **Advanced AI Techniques:**
  - **Federated Learning:** Training AI models on decentralized data without sharing raw data, enhancing privacy.
  - **Reinforcement Learning:** Optimizing supply chain decisions (e.g., routing, inventory) based on real-time feedback and detected anomalies.
  - **Explainable AI (XAI):** Developing techniques to make AI-driven anomaly detections more transparent and understandable.
- **Decentralized Autonomous Organizations (DAOs):** Exploring DAOs for governing certain aspects of the supply chain network.
- **Cross-Chain Interoperability Solutions:** Developing and adopting protocols that allow seamless communication and data exchange between different blockchain platforms.
- **Development of Industry-Specific Standards:** Creating common frameworks and data models for blockchain and AI in SCM for various sectors.
- **Sustainability Tracking:** Using the platform to track and verify sustainability metrics (e.g., carbon footprint, ethical sourcing) throughout the supply chain.

SJIF Impact Factor (2025): 8.688| ISI I.F. Value: 1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 10 | Issue: 5 | May 2025 - Peer Reviewed Journal

7. CONCLUSION

The integration of blockchain technology with AI/ML-driven anomaly detection systems offers a paradigm shift for Supply Chain Management. Blockchain provides a foundational layer of trust, security, and transparency by creating an immutable and shared record of transactions and product journeys. Layered on top, AI and ML algorithms, implemented using versatile tools like Python, can intelligently sift through this data to proactively identify anomalies, predict disruptions, and flag potential fraud.

This synergistic approach addresses many of the critical pain points of traditional supply chains, leading to enhanced security, improved efficiency, greater transparency, and proactive risk management. While challenges related to scalability, interoperability, cost, and adoption exist, the potential benefits are compelling enough to drive continued research and development.

As these technologies mature and standards evolve, the vision of a truly intelligent, self-regulating, and secure supply chain moves closer to reality. The integrated system proposed in this paper provides a conceptual framework for harnessing the combined power of blockchain and AI/ML to build more resilient and trustworthy global supply networks, ultimately benefiting businesses, consumers, and the global economy.

8. REFERENCES

1. *Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys (CSUR), 41(3), 1-58.*
2. *Fildes, R., Goodwin, P., Lawrence, M., & Nikolopoulos, K. (2008). Effective forecasting and judgmental adjustments: an empirical evaluation and strategies for improvement in supply-chain planning. International Journal of Forecasting, 24(1), 3-23.*
3. *Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.*
4. *Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of the literature. Decision Support Systems, 50(3), 559-569.*
5. *Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117-2135.*
6. *Tijan, E., Aksentijević, S., Ivanić, K., & Jardas, M. (2019). Blockchain technology implementation in logistics. Sustainability, 11(4), 1185.*
7. *Hyperledger Foundation. (Various years). Hyperledger Fabric Documentation. [Online]. Available: hyperledger.org/projects/fabric*
8. *Scikit-learn Development Team. (Various years). Scikit-learn: Machine Learning in Python. [Online]. Available: scikit-learn.org*
9. *TensorFlow Development Team. (Various years). TensorFlow. [Online]. Available: tensorflow.org*