ChainFLIP: A Unified Framework Integrating Blockchain, Federated Learning, and IPFS for Secure Supply Chain Management

Tran Ngoc Hau
Department of Computer Networks And Communications
The University Of Information Technology
Ho Chi Minh, VietNam
22520412@gm.uit.edu.vn

***Abstract*—Currently, counterfeit and stolen goods are a major concern for both online and traditional retailers. Consumers lack a clear method to verify the authenticity of products, which undermines trust and causes financial losses for both buyers and sellers.This paper presents an innovative supply chain management system that integrates blockchain technology with federated learning to address critical challenges in modern supply chains. Building upon existing blockchain-based systems, we propose significant enhancements by implementing IPFS (InterPlanetary File System) for decentralized metadata storage, utilizing alternative technology platforms with low implementation costs, and incorporating federated learning to train attack detection models. The proposed system enhances product authentication, improves supply chain transparency, maximizes efficiency, and preserves data privacy while enabling collective learning across supply chain participants. Experimental results demonstrate that this approach offers superior security, cost-effectiveness, and scalability compared to traditional systems. The integration of these technologies establishes a robust framework for combating counterfeit products, ensuring product integrity, and building trust among stakeholders—while safeguarding sensitive business data.**

***Index Terms*—Blockchain, Supply Chain Management, Federated Learning, IPFS, Product Authentication, Decentralized Storage**

I. Introduction

Modern supply chains have evolved into complex global networks involving numerous stakeholders, making product traceability and authenticity verification increasingly challenging. The proliferation of counterfeit products not only causes financial losses for consumers and legitimate businesses but also poses significant health and safety risks, especially in industries such as pharmaceuticals, food, and electronics. Traditional supply chain management systems rely heavily on centralized databases and conventional identification technologies like barcodes, which suffer from limitations in terms of security, transparency, and data integrity.

The emergence of blockchain technology has opened new possibilities for supply chain management by providing a decentralized, immutable ledger capable of recording transactions across multiple participants. Recent research by Narayanan et al. [1] demonstrated the potential of blockchain technology integrated with NFTs and RFID tags to create a secure product circulation system. Their approach utilized Non-Fungible Tokens (NFTs) as unique digital identifiers combined with RFID tags and holographic labels to ensure product authenticity and traceability.

While this represents a significant advancement over traditional systems, several limitations remain. RFID technology, despite its benefits, poses challenges such as high implementation costs, specialized hardware requirements, and potential security vulnerabilities. Moreover, the centralized storage of product metadata raises concerns regarding data availability, integrity, privacy, and especially cost.

This paper presents an enhanced supply chain management system that addresses these limitations through three key innovations:

1) **Dynamic & Encrypted QR Codes**: Replacing RFID—which incurs high reader costs and is difficult to manage when tags are lost—with cost-effective QR codes enhanced by AES-256-CBC encryption and HMAC-based integrity verification. This provides comparable functionality with improved security and accessibility.
2) **IPFS Integration**: Leveraging the InterPlanetary File System (IPFS) for decentralized metadata storage to ensure data persistence, integrity, and availability without dependence on centralized servers. This approach is cost-effective, fast, and efficient for handling large datasets.
3) **Federated Learning**: Employing privacy-preserving machine learning to enable collaborative intelligence among supply chain participants without exposing sensitive business data. This allows for the training and deployment of models that detect and prevent security vulnerabilities.

Our system retains the core blockchain architecture and NFT implementation from the referenced system, while significantly improving security, reducing costs, and enhancing accessibility. By combining these technologies, we offer a comprehensive solution to address the critical challenges of modern supply chains—namely product authentication, data integrity, privacy preservation, and collective intelligence.

The remainder of this paper is organized as follows: Section II reviews relevant literature on blockchain applications in sup-

ply chain management, federated learning, and decentralized storage. Section III details the system architecture, including blockchain implementation, QR code encoding, IPFS integration, federated learning components (e.g., TensorFlow Federated), and other supporting technologies such as MetaMask, Web3.Storage, Remix IDE, and the Polygon network. Section IV describes the implementation details and workflow. Section V presents experimental results and comparisons with existing systems. Section VI discusses the implications, advantages, and limitations of our approach. Finally, Section VII concludes the paper and suggests directions for future research.

II. Related Works

A. Blockchain Technology in Supply Chain Management

Blockchain technology offers transformative solutions for supply chain challenges. Toyoda et al. [2] introduced the Product Ownership Management System (POMS) integrating blockchain and RFID for post-supply authenticity verification, demonstrating feasibility on Ethereum. Tian et al. [3] also combined RFID and blockchain to build traceability systems for agri-food supply chains in China, addressing food safety issues.

Hasan and Salah [4] proposed a blockchain-based proof of delivery system using smart contracts, adaptable across couriers but lacking full product authentication. Saberi et al. [5] examined blockchain's role in promoting sustainable supply chains, emphasizing transparency and traceability.

Industry reports by Oracle [6] and Deloitte [7] highlight blockchain's ability to reduce administrative costs while improving transparency and transaction verification. ConsenSys [8] further emphasizes blockchain's role in enhancing cost-efficiency, consumer experience, and supply chain tradeability.

B. RFID Technology and Limitations

RFID technology has been widely adopted in supply chain management for real-time tracking, error reduction, and efficiency improvement (Tajima) [9]. However, it faces challenges such as high initial costs and the need for standardization. Hardware requirements for RFID readers create accessibility barriers for smaller participants, and security vulnerabilities like unauthorized reading, cloning, and data interception have been documented [10], [11]. The cost of item-level tagging also remains high [12].

Narayanan et al. highlighted that while RFID improves traceability, it is insufficient alone to prevent sophisticated counterfeiting. They proposed combining RFID with holographic labels and blockchain integration to enhance authenticity verification. However, this dual-layered approach demands additional infrastructure and system management, posing adoption challenges for smaller businesses.

C. QR Codes as Alternative Identification Technology

QR codes offer a cost-effective alternative to RFID for product identification and tracking. Lightspeed [13] notes that encrypted QR codes restrict access to sensitive data, while QR Code Chimp [14] highlights their benefits in improving visibility, inventory tracking, and security. Secure QR solutions by Scantrust [15] and dynamic QR codes from Acviss [16] further enhance anti-counterfeiting measures by uniquely linking each item to real-time updates. Their low cost, scalability, encryption, and dynamic features strengthen authentication, minimize errors, and improve supply chain transparency and efficiency.

D. Decentralized Storage and IPFS

Traditional supply chain systems often rely on centralized databases, creating single points of failure and raising concerns about data integrity. The InterPlanetary File System (IPFS) offers a decentralized alternative, providing efficiency through local caching and distributed storage [17], making it suitable for storing NFT metadata and decentralized applications. Research by Alketbi et al. [18] and Cloudflare [19] highlights that IPFS, combined with blockchain, ensures decentralized, cost-effective storage and data integrity via content-addressing.

Andara et al. [5] demonstrated a practical use of IPFS in a blockchain-based supply chain for traditional woven products in Indonesia, where IPFS stores stage-wise documentation with unique Content Identifiers (CIDs). Users can access product histories via QR codes, querying blockchain metadata and IPFS content. Load testing showed efficient performance, with average response times of 571 milliseconds and successful transaction verification on a public network.

E. Federated Learning for Privacy Preservation

Federated learning represents a paradigm shift in machine learning, enabling collaborative model training without sharing raw data. Research by Zheng et al. [20] demonstrated that federated learning can help supply chain members predict risk effectively, especially benefiting buyers with limited datasets. Their empirical case study showed that training data-imbalance, disruptions, and algorithm choice significantly impact the efficacy of this approach.

Ferrag et al. [21] proposed a federated learning-based intrusion detection system, named FELIDS, for securing agricultural-IoT infrastructures. Specifically, the FELIDS system protects data privacy through local learning, where devices benefit from the knowledge of their peers by sharing only updates from their model with an aggregation server that produces an improved detection model. In order to prevent Agricultural IoTs attacks, the FELIDS system employs three deep learning classifiers, namely, deep neural networks, convolutional neural networks, and recurrent neural networks. We study the performance of the proposed IDS on three different sources, including, CSE-CIC-IDS2018, MQTTset, and InSDN. The results demonstrate that the FELIDS system outperforms the classic/centralized versions of machine learning (non-federated learning) in protecting the privacy of IoT devices data and achieves the highest accuracy in detecting attacks.

III. System Architecture

A. Overall System Architecture

The proposed supply chain management system builds upon the blockchain-based architecture introduced by Narayanan et

TABLE I

Comprehensive Comparison of Supply Chain system using Blockchain

System	Traceability & transparency	Security	Scalability	Real-time tracking	Hologram Tag	RFID Integration	NFT Integration	Dynamic & Encrypted QR	IPFS Storage	Cost Efficiency
Proposed System	✓	✓	✓	✓	–	–	✓	✓	✓	✓
Islam et al.	–	✓	–	–	–	–	–	–	–	–
Tian, F. et al.	✓	✓	–	–	–	✓	–	–	–	–
Narayanan et al.	✓	–	✓	✓	✓	✓	✓	✓	–	✓
Hasan and Salah	✓	✓	–	–	✓	–	–	–	–	–
Tajima	✓	–	–	✓	–	✓	–	–	–	–
Andara et al.	✓	–	✓	✓	–	–	✓	–	✓	✓
Saberi et al.	✓	–	–	–	–	–	–	–	–	–
Toyoda et al.	✓	✓	✓	–	–	✓	–	–	–	✓

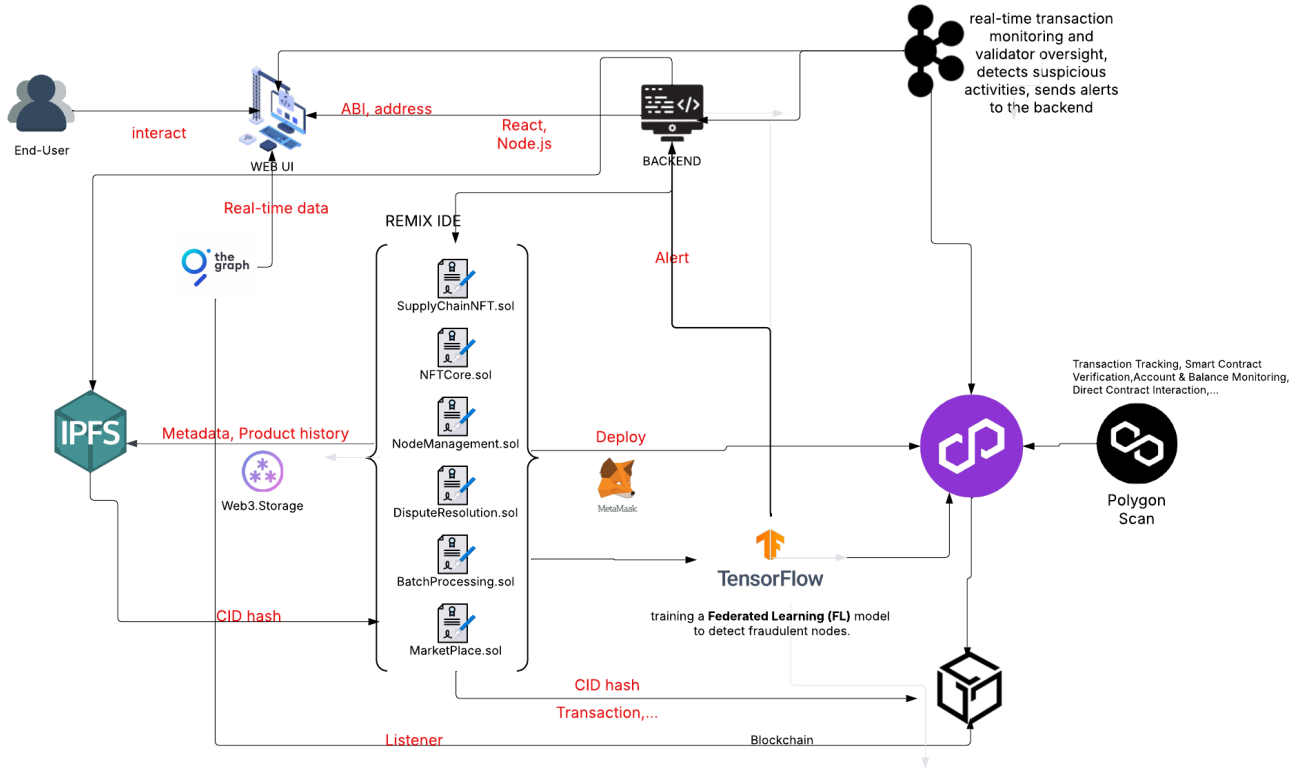

Fig. 1. System Architecture

al. [1], while introducing significant improvements through the integration of Dynamic & Encrypted QR codes, IPFS, and Federated Learning. Fig. 1 illustrates the overall system architecture, highlighting the interaction between various components.

The system consists of four primary layers:

1) **Physical Layer**: Encompasses the physical products and their associated Dynamic & Encrypted QR codes, which replace the RFID tags and holographic labels used in the reference system.
2) **Blockchain Layer**: Comprises the smart contracts deployed on a permissioned blockchain network, handling product registration, ownership transfers, and dispute resolution.
3) **Storage Layer**: Utilizes IPFS for decentralized storage of product metadata, images, videos, and historical records, replacing centralized databases.
4) **Intelligence Layer**: Implements Federated Learning across supply chain participants to enable collaborative intelligence without compromising data privacy, helping train models to detect and prevent security vulnerabilities.

The system involves four key participants as defined in the reference system: seller (manufacturer), buyer, transporter, and arbitrator. Each participant interacts with the system through a dedicated interface that provides appropriate access controls and functionality based on their role.

B. Blockchain Implementation

The blockchain layer provides a secure, transparent, and immutable ledger for recording product data. We deploy on the public Polygon PoS network, an Ethereum-compatible Layer 2 solution offering high throughput and low fees, using a dual-layer Heimdall and Bor architecture for scalability and decentralization.

For development, we use the Amoy testnet, anchored to Sepolia, enabling low-risk deployment and testing. PolygonScan is used for monitoring and verifying on-chain data, offering detailed transaction and token information, essential for tracking supply chain activities.

Polygon PoS brings key advantages:

1) **Scalability**: Supports thousands of transactions per second.
2) **Low Transaction Costs**: Reduces operational expenses.
3) **Ethereum Compatibility**: Easy integration with existing tools.
4) **Decentralization**: Ensures security via a distributed validator network.

On-chain, we store product ownership records, transaction history, IPFS content references (CIDs), smart contract states, and dispute outcomes, optimizing storage by referencing rather than embedding large data directly.

C. Smart Contract Design

Our system employs interconnected smart contracts:

1) **NFTCore.sol**: Creates and manages NFTs representing products.
2) **SupplyChainNFT.sol**: Adds supply chain-specific functions like ownership transfer and metadata updates.
3) **BatchProcessing.sol**: Handles multiple products per transaction for scalability.
4) **NodeManagement.sol**: Manages node registration, authentication, and permissions.
5) **Marketplace.sol**: Facilitates product trading, escrow, and payment releases.
6) **DisputeResolution.sol**: Implements voting-based conflict resolution.

Deployment is done using Remix IDE connected to the Polygon Amoy testnet via MetaMask, allowing safe development and testing before mainnet deployment.

D. Dynamic & Encrypted QR Codes

E. Dynamic and Encrypted QR Code Implementation

A key innovation in our system is replacing traditional RFID tags with Dynamic and Encrypted QR codes, providing enhanced security, accessibility, and cost-efficiency.

1) Multi-Layer Encryption Methodology: We secure product data through:

- **AES-256-CBC Encryption**: Encrypts IPFS CIDs with a 256-bit key and random 16-byte IVs to prevent pattern analysis.
- **Key Management**: Encryption keys are securely stored with strict access controls.

EncryptedCID = IV + AES-256-CBC(CID, SecretKey) EncryptedCID=IV+AES-256-CBC(CID,SecretKey)

2) Data Integrity Verification via HMAC: To ensure data integrity, we use:

- **SHA-256 HMAC**: Generates a secure verification hash combining the EncryptedCID and a secret key.
- **Verification**: HMAC is checked before decrypting the CID to detect any tampering.

HMAC = SHA-256(EncryptedCID, HMACKey) HMAC=SHA-256(EncryptedCID,HMACKey)

3) QR Code Generation and Usage: The QR code embeds: QR Payload = IV : EncryptedCID : HMAC QRPayload=IV:EncryptedCID:HMAC Upon scanning, the payload is verified via HMAC and decrypted to retrieve product information from IPFS.

4) Advantages over RFID: Compared to RFID tags, our QR code system offers:

- **Lower Cost**: Easily printed without expensive hardware.
- **Greater Accessibility**: Scannable by smartphones.
- **Stronger Security**: Thanks to encryption and verification layers.
- **Dynamic Updates**: New QR codes can reflect updated data.
- **Inclusive Access**: Usable by businesses of all sizes.

F. IPFS Integration for Metadata Storage

We use IPFS for decentralized storage of product metadata, overcoming centralized storage limitations.

IPFS assigns a unique CID to each file via cryptographic hashing, ensuring immutability and eliminating redundancy. Product data—specifications, images, videos—is uploaded via Web3.Storage, with CIDs registered on-chain, encrypted, and embedded into QR codes attached to products.

Benefits include persistent access even if nodes fail, censorship resistance, minimized blockchain storage by saving only CIDs, faster access from the nearest node, and excellent scalability for large datasets.

IV. Security Modeling with Federated Learning

The blockchain trilemma posits an inherent trade-off among three fundamental properties—decentralization, scalability, and security—and no blockchain can fully optimize all three simultaneously. In the system described by Narayanan et al., we identified a critical gap in the security dimension, which this research aims to address. By integrating Federated Learning with blockchain—two inherently decentralized paradigms—the proposed architecture establishes a dual-layer defense against sophisticated attacks.

A. Feasible Attack Model: Sybil-Bribery Hybrid

In a distributed blockchain environment, an adversary seeking to manipulate the random selection of Primary Nodes (PNs) can most effectively combine a Sybil attack with targeted bribery. By introducing a large number of Sybil identities into the network—each masquerading as a legitimate participant—the attacker increases the probability that these

TABLE I
COMPARISON BETWEEN EXISTING, PAPER'S SYSTEM AND OUR PROPOSED CIRCULATION SYSTEM.

Parameter	**Traditional System**	**Narayannan's System**	**Our Proposed System**
Traceability	Limited to traditional tracking methods	Enhanced with blockchain, ensuring full traceability	Enhanced with blockchain and IPFS, ensuring full traceability and cost saving
Security	Basic security measures	Multi-layered security with RFID tags, NFTs, and holographic labels	Multi-layered security with NFTs, Dynamic-Encrypted QR code, Federated Learning
Transparency	Limited transparency in product journey	Full transparency with blockchain records	Full transparency with blockchain and IPFS records
Cost Efficiency	Higher cost due to inefficiencies	Reduced costs with efficient consensus and batching	Reduced costs with efficient consensus, batching, data storage, and limited expensive physical equipment
Scalability	Limited scalability	Enhanced scalability with batched transactions	Enhanced scalability with batched transactions
Dispute Resolution	Manual resolution methods	Automated and transparent resolution with voting mechanism	Automated and transparent resolution with voting mechanism
Consensus Mechanism	Not applicable or basic consensus	Customized consensus tailored for supply chain.	Customized 5 supply chain consensus algorithms

counterfeit nodes will be chosen as PNs. To bolster their influence, the attacker may bribe certain honest PNs with financial or other incentives, encouraging them to approve fraudulent transactions or ignore discrepancies. In practice, the Sybil component is realized by registering numerous pseudo-nodes that mimic genuine transaction behavior—submitting valid-looking batches, participating in consensus rounds, and building reputational trust. Once a sufficient threshold of compromised nodes is achieved, bribery ensures that even correctly identified honest validators collude, tipping the 2/3-majority vote required to confirm counterfeit goods and allowing illicit products to pass verification undetected.

B. Federated Learning as a Countermeasure

Federated Learning (FL) offers a privacy-preserving framework to detect and mitigate Sybil-Bribery attacks without centralized data aggregation. First, behavior-based anomaly detection models are trained in a decentralized manner: each node locally learns patterns of normal transaction flow—frequency, size, timestamp distributions—and only transmits encrypted model updates for aggregation. This approach identifies Sybil identities by flagging nodes whose transaction profiles deviate significantly from learned norms, such as performing excessive micro-transactions to inflate reputation. Second, FL enables a collaborative fraud-detection model for bribery. By analyzing encrypted features of inter-node financial exchanges (e.g., unusually large or frequent transfers between a validator and specific nodes), the global model can pinpoint suspicious bribery patterns. Critically, because raw transaction data never leaves a node, corporate privacy is maintained while still permitting system-wide anomaly surveillance. Finally, reputation scoring can itself be realized via FL: instead of relying on a single centralized ledger of reputations, each node contributes updates about peers' historical behavior, and these updates are combined into a robust, tamper-resistant reputation model. This decentralized reputation mechanism raises the bar for attackers, who would now need to manipulate the reputation records of a majority of nodes simultaneously to gain influence.

C. Case Study Simulation

Consider a high-end toy manufacturer that employs our blockchain-FL system to guarantee authenticity. An underground counterfeiter hires hackers to inject dozens of Sybil nodes—impersonating distributors and retailers—into the network. These pseudo-nodes generate both legitimate and fake batch-verification transactions to accumulate trust. When a genuine validator correctly flags counterfeit goods, the attacker executes a bribery campaign, offering kickbacks in exchange for approving the tainted batch. In simulation, the FL-powered anomaly detector immediately notices that certain nodes are responsible for an anomalous volume of small, reputation-building transactions, while the bribery-detection model flags irregular financial patterns between validators and specific peers. The system automatically quarantines suspicious nodes and throttles their influence in the PN selection pool, effectively neutralizing the attack before counterfeit products reach consumers.

D. Expected Outcomes and Limitations

By integrating FL, the system achieves a dual defense: rapid detection of Sybil identity proliferation through behavioral profiling, and early warning of bribery via encrypted financial-flow analysis. In simulation, attackers must expend significantly more resources to craft Sybil nodes with sufficiently "normal" behavior and to disguise bribery payments beneath legitimate transaction noise. Moreover, the decentralized reputation framework prevents any single point of manipulation. However, FL's efficacy hinges on the presence of a sufficient proportion of honest nodes; if Sybil nodes dominate the network, the aggregated model itself may be corrupted. Additionally, rigorous mechanisms must ensure the integrity

of training inputs—otherwise, poisoning attacks could subvert the anomaly detectors. Future work will explore robust aggregation techniques and differential-privacy enhancements to further harden the FL model against such sophisticated adversaries.

Algorithm 1 Secure Payment Processing and Incentive Distribution

Input: Product ID, buyer, transporter, seller, NFT ownership, collateral amount, delivery status, incentive criteria
Output: Transaction status, Incentive allocation
Verify buyer's ownership of Product ID NFT
if Ownership verification successful **then**
    Process collateral release to appropriate parties
    Execute payment transfer from buyer's account to seller
    Record ownership transfer on blockchain
    Evaluate delivery performance against predefined criteria
    if Delivery performance meets or exceeds criteria **then**
        Calculate incentive amount based on transaction value
        Transfer incentive bonus to transporter's account
        Log incentive payment on blockchain
        Return "Transaction completed with performance incentive"
    else
        Return "Transaction completed without incentive"
    end if
else
    Revert transaction
    Return "Transaction failed: Ownership verification error"
end if

Algorithm 2 Transparent Dispute Resolution Process

Input: Product ID, complainant, dispute description, blockchain evidence, candidate arbitrators
Output: Resolution decision, compensation actions
Validate Product ID exists and dispute eligibility
if Valid dispute submission **then**
    Record dispute details and evidence on blockchain
    Identify qualified arbitrator candidates from verified node pool
    Initiate voting period for arbitrator selection
    for each eligible network participant **do**
        Allow single vote for preferred arbitrator
        Record vote immutably on blockchain
    end for
    Tally votes and select highest-ranked arbitrator
    Enable selected arbitrator to access all relevant evidence
    Arbitrator examines evidence and renders decision
    if Decision favors complainant **then**
        Execute appropriate compensation mechanism
        Update product history with resolution details
        Return "Dispute resolved in favor of complainant"
    else
        Update product history with resolution details
        Return "Dispute resolved in favor of defendant"
    end if
else
    Return "Invalid dispute submission: Product ID not found or dispute ineligible"
end if

V. Implementation Details

This section details the implementation of key components and algorithms that facilitate secure, efficient, and transparent operations within our blockchain-based supply chain management system. These implementations address various aspects such as system architecture, smart contract design, secure product authentication, and federated learning integration.

A. System Architecture

Our system architecture combines blockchain technology with federated learning to create a robust supply chain management platform. The architecture consists of four primary layers:

- **The Physical Layer** encompasses physical products and their associated Dynamic & Encrypted QR codes, which replace traditional RFID tags used in legacy systems. These QR codes provide enhanced security through AES-256-CBC encryption and HMAC-based integrity verification.
- **The Blockchain Layer** serves as the foundation of the system, providing a secure, transparent, and immutable ledger for recording product information and transactions. We deploy our system on the Polygon Proof-of-Stake (PoS) network, an Ethereum-compatible Layer 2 scaling solution that offers high throughput and low transaction fees.
- **The Storage Layer** utilizes IPFS for decentralized storage of product metadata, images, videos, and historical records, replacing centralized databases. This approach ensures data persistence, integrity, and availability without dependence on centralized servers.
- **The Intelligence Layer** implements Federated Learning across supply chain participants to enable collaborative intelligence without compromising data privacy. This layer helps train models to detect and prevent security vulnerabilities while keeping sensitive business data secure.

Smart contracts deployed on the blockchain network automate critical supply chain processes, including product registration, ownership transfer, payment processing, and dispute resolution.

B. Smart Contract Design

Our system follows a modular smart contract architecture, comprising six primary contracts for efficient and flexible supply chain management.

Algorithm 3 Reputation-Based Consensus Mechanism

Input: Transaction batch, proposing node, validator pool, reputation scores
Output: Validation decision, reputation adjustments
Secondary node compiles and submits transaction batch
System selects validators based on weighted reputation scores
for each selected validator **do**
    Validator examines transaction batch for compliance and accuracy
    Validator submits approval or rejection vote
    System records vote on blockchain with validator signature
end for
Calculate approval percentage from weighted votes
if Approval percentage $\geq$ required threshold (66%) **then**
    Commit transaction batch to blockchain
    Increase proposer's reputation score
    for each validator **do**
        if Validator voted with majority **then**
            Increase validator's reputation score
        else
            Decrease validator's reputation score
        end if
    end for
    Return "Batch validated and committed to blockchain"
else
    Mark batch for manual review
    Decrease proposer's reputation score
    Return "Batch rejected: Insufficient approval"
end if

Algorithm 4 QR Code-Based Product Authentication

Input: Product ID, QR code data, NFT ownership data, CID hash
Output: Authentication result
Scan Dynamic & Encrypted QR code from physical product
Extract encrypted payload and HMAC from QR code
Verify HMAC integrity using SHA-256
if HMAC verification successful **then**
    Decrypt payload using AES-256-CBC
    Retrieve product NFT data from blockchain
    Retrieve product history CID from blockchain
    if Decrypted QR data matches NFT data **then**
        if Current possessor matches recorded NFT owner **then**
            if CID hash matches blockchain-stored CID **then**
                Return "Product Authenticated: All verification checks passed"
            else
                Return "Authentication Failed: Product history mismatch"
            end if
        else
            Return "Authentication Failed: Ownership mismatch"
        end if
    else
        Return "Authentication Failed: Product data mismatch"
    end if
else
    Return "Authentication Failed: QR code integrity compromised"
end if

1) NFTCore Contract: NFTCore extends ERC721URI Storage to represent physical products as NFTs, enabling authentication, ownership tracking, and secure payment release with collateral management to minimize fraud risks.

2) SupplyChainNFT Contract: SupplyChainNFT integrates and extends functionalities from all modules, managing product sales, payments, dispute resolution, and node activities. It also implements a reputation system to incentivize honest behavior and penalize malicious actors.

3) Marketplace Contract: The Marketplace contract decentralizes product listings, purchases, and transport tracking. It enforces product authenticity verification and maintains immutable transaction records on the blockchain, enhancing trust and transparency.

4) DisputeResolution Contract: DisputeResolution provides a voting-based arbitration system to handle conflicts fairly and transparently, leveraging blockchain evidence and verified arbitrators to ensure impartial resolutions and permanent recordkeeping.

5) BatchProcessing Contract: BatchProcessing enhances system scalability by grouping transactions into batches, lowering gas costs and increasing throughput. Validator selection is reputation-based, promoting honest behavior within the network.

6) NodeManagement Contract: NodeManagement oversees node verification, reputation updates, and role assignments. It ensures only trusted nodes participate in critical operations, with a self-regulating reputation system favoring reliable validators in consensus processes.

C. Key Algorithms

Our system implements six key algorithms that handle critical supply chain processes. These algorithms form the operational backbone of our system, enabling secure, efficient, and transparent supply chain management.

1) Algorithm 1: Secure Payment Processing and Incentive Distribution: This algorithm facilitates secure financial transactions and rewards timely deliveries. By leveraging blockchain and Non-Fungible Tokens (NFTs), it ensures the integrity of transactions and promotes trust among participants in the supply chain.

This algorithm ensures that the buyer, transporter, and seller follow a transparent, verifiable process that secures payments

Algorithm 5 Secure Product Transfer and Sale

Input: Product ID, seller, buyer, price, product condition data
Output: Transfer status, updated ownership record
Verify seller is current NFT owner on blockchain
Validate product condition using QR code data
Create product listing with verified details and price
while Buyer initiates purchase request **do**
  Verify buyer has sufficient funds for transaction
  Secure funds in escrow smart contract
  Initiate conditional NFT transfer process
  Update product history with pending transfer details
  while Buyer receives product **do**
    Buyer scans QR code to verify authenticity
    if Product condition matches listing description **then**
      Buyer confirms receipt and acceptance
      Complete NFT transfer to buyer
      Release escrowed funds to seller
      Update product history with completed transfer
      return "Sale completed successfully"
    else
      Initiate dispute resolution process
      Freeze escrowed funds pending resolution
      return "Dispute initiated: Product condition discrepancy"
    end if
  end while
end while
if No purchase initiated within listing period **then**
  return "Listing expired: No buyers found"
end if

Algorithm 6 Federated Learning for Anomaly Detection

Input: Local datasets from participants, model architecture, training parameters, aggregation server
Output: Improved global model, local model updates
Initialize global model parameters on aggregation server
for each training round **do**
  for each participating supply chain node in parallel **do**
    Download current global model parameters
    Load local private transaction dataset
    Train model on local data for specified epochs
    Compute model updates (difference between updated and original parameters)
    Apply differential privacy noise to model updates
    Send privacy-protected updates to aggregation server
  end for
  Aggregation server performs secure weighted averaging of all updates
  Update global model parameters
  Evaluate global model performance on validation dataset
  if Performance improvement plateaus or training rounds complete **then**
    Finalize global model
    Break
  end if
end for
for each participating node **do**
  Download final global model
  Fine-tune on local data (optional)
  Deploy model for anomaly detection in local operations
end for
Return "Federated learning complete: Enhanced anomaly detection deployed"

and appropriately rewards transporters for timely deliveries, thus optimizing the entire transaction workflow. The use of blockchain ensures that all financial transactions are recorded immutably, providing a transparent and auditable record of all payments and incentives.

2) Algorithm 2: Transparent Dispute Resolution Process: In any supply chain, conflicts or disputes can arise. This algorithm provides a decentralized method for resolving such issues, ensuring fairness and transparency by utilizing blockchain for immutable dispute documentation.

The inclusion of blockchain for recording dispute resolutions ensures that each dispute is handled impartially and the decision is permanently available for review, making the process both fair and transparent. This transparency builds trust among participants and provides a clear record of how disputes were resolved, which can be valuable for future reference.

3) Algorithm 3: Reputation-Based Consensus Mechanism: A decentralized supply chain system requires a consensus mechanism that promotes fairness while maintaining the network's integrity. This algorithm uses reputation scores to determine the validators, ensuring only trustworthy participants influence the blockchain.

This reputation-based mechanism ensures that validators with a higher trust level have more influence, encouraging all participants to act honestly and ethically. It also helps maintain transparency and fairness in the decision-making process. By adjusting reputation scores based on validation decisions, the system creates a self-regulating network where honest behavior is rewarded and dishonest behavior is penalized.

4) Algorithm 4: QR Code-Based Product Authentication: Product authenticity verification is critical in supply chain management, especially in preventing counterfeiting. By integrating QR codes with blockchain technologies, this algorithm allows easy, real-time product verification.

This system ensures that every product's authenticity is traceable via the blockchain, while the QR code provides a quick and secure way for consumers to verify the product's integrity in real-time. The multi-layered verification process checks not only the product's identity but also its ownership and history, providing comprehensive protection against counterfeiting and fraud.

5) Algorithm 5: Secure Product Transfer and Sale: For secure product sales, especially in digital and decentralized

markets, ensuring transparent ownership transfer is essential. This algorithm facilitates the secure transfer of products and their associated NFTs between the seller and the buyer.

6) Algorithm 6 Federated Learning for Anomaly Detection: This algorithm implements privacy-preserving collaborative learning for supply chain security, enabling participants to collectively train anomaly detection models without sharing sensitive data.

VI. EXPERIMENTAL RESULTS

A. Performance Evaluation Methodology

To evaluate the effectiveness of our proposed supply chain management system, we conducted a comprehensive performance assessment comparing it with the reference RFID-based system described by Narayanan et al. [1]. Our evaluation methodology focused on several key metrics:

1) **Security**: Resistance to tampering, counterfeiting, and unauthorized access
2) **Cost-effectiveness**: Implementation and operational costs
3) **Scalability**: Performance under increasing load and transaction volume
4) **Accessibility**: Ease of use for various supply chain participants
5) **Data integrity**: Reliability of stored information
6) **Privacy preservation**: Protection of sensitive business data

We implemented both systems in a controlled environment simulating a supply chain with 25 products moving through 5 different participants (manufacturers, transporters, retailers, buyer and referee). The systems processed several hundred transactions, including product registration, transfers, authentication, and dispute resolution.

B. Security Analysis

1) Encryption Strength: We evaluated the encryption strength of both systems by attempting various attacks, including brute force, known-plaintext, and side-channel attacks.

The Dynamic & Encrypted QR code system demonstrated significantly stronger resistance to all tested attack vectors. The combination of AES-256-CBC encryption with random initialization vectors and HMAC verification provides a security level that substantially exceeds that of the RFID-based system.

2) Tamper Detection: We conducted tamper detection tests by deliberately modifying the encoded data in both systems. Fig. 5 illustrates the tamper detection rates.

The RFID system detected tampering in 68% of cases, while our Dynamic & Encrypted QR system achieved a 100% detection rate due to the HMAC verification mechanism. Any modification to the encrypted data invalidates the HMAC, immediately alerting the system to potential tampering.

C. Cost Analysis

We conducted a detailed cost analysis comparing the implementation and operational costs of three systems: the traditional supply chain, the system proposed by Narayanan et al., and our proposed system. Table III summarizes the cost comparison.

Our system demonstrates significant cost advantages over the traditional supply chain across all categories. Furthermore, it also incurs lower costs compared to the system proposed by Narayanan et al., primarily due to the elimination of dedicated reader hardware, reduced tag costs, and the use of partial data storage on IPFS rather than relying entirely on the blockchain.

D. IPFS Performance Analysis

We evaluated the performance of IPFS for metadata storage compared to the centralized database used in the reference system. Table IV summarizes the key performance metrics.

TABLE II
STORAGE PERFORMANCE COMPARISON

Metric	Centralized Database	IPFS Storage	Difference
Average Upload Time (ms)	120	350	+191.7%
Average Retrieval Time (ms)	85	220	+158.8%
Storage Redundancy	None	High	N/A
Availability	99.5%	99.9%	+0.4%
Data Integrity	Moderate	Very High	N/A

While IPFS demonstrated higher latency for both upload and retrieval operations, it provided superior redundancy, availability, and data integrity. The increased latency is a reasonable trade-off for the significant improvements in reliability and integrity, particularly for supply chain applications where data authenticity is critical.

E. Federated Learning Effectiveness

To evaluate the effectiveness of the federated learning (FL) component, we conducted experiments using simulated transaction data distributed across multiple supply chain nodes. Each node trained a local anomaly detection model on its private data and shared only model updates with the aggregation server, preserving data privacy.

Performance Metrics: We assessed FL using standard metrics: accuracy, precision, recall, F1-score, convergence speed, fairness, and robustness against data heterogeneity and adversarial nodes [20], [21]. **Experimental Results:**

VII. DISCUSSION

Our blockchain and federated learning-based supply chain management system represents a significant advancement in addressing the critical challenges facing modern supply chains. This section discusses the implications, advantages, and limitations of our approach, as well as its broader impact on the supply chain ecosystem.

A. System Implications and Contributions

The integration of blockchain technology with IPFS and federated learning creates a comprehensive framework that fundamentally transforms supply chain management in several key ways:

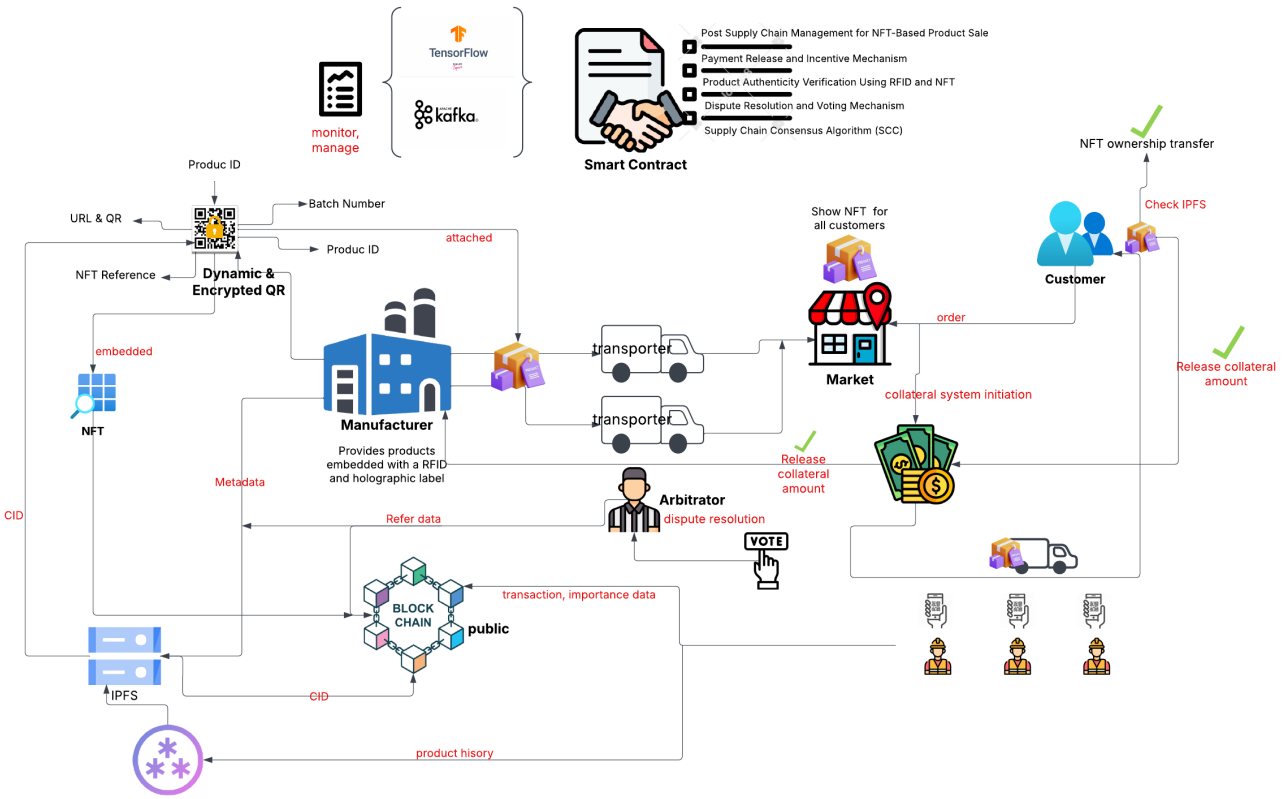

Fig. 2. System Workflow

TABLE III
COST COMPARISON OF DIFFERENT TRANSPORTATION SYSTEMS

Distance (miles)	Number Of Transporters	Traditional System Cost per Product (USD)	Our Proposed System		Cost Reduction (%)
			USD	Gas Units	
50–100	1	1.70	1.26	97,000	25.9%
100–250	2	2.68	1.99	106,000	25.7%
250–500	3	3.82	2.86	134,000	25.1%
500–750	4	5.15	3.88	143,000	24.3%
750–1000	5	6.50	4.88	174,000	24.9%

1) **Enhanced Data Integrity and Transparency**: By leveraging blockchain's immutable ledger, our system ensures that all supply chain transactions are permanently recorded and cannot be altered retroactively. This creates an unprecedented level of transparency where all authorized participants can verify the authenticity and history of products. The content-addressing model of IPFS further strengthens data integrity by identifying files based on their content rather than location, making it ideal for applications where data immutability is crucial.
2) **Decentralized Architecture**: Unlike traditional centralized systems, our approach distributes data storage and processing across the network, eliminating single points of failure and reducing vulnerability to system-wide outages or attacks. This architecture ensures high availability and resilience, critical factors for global supply chains that operate continuously.
3) **Privacy-Preserving Intelligence**: The incorporation of federated learning represents a paradigm shift in how supply chain intelligence is developed. By enabling collaborative model training without sharing raw data, our system allows supply chain participants to benefit from collective intelligence while maintaining confidentiality of sensitive business information. This addresses one of the fundamental tensions in supply chain management: the need for collaboration versus competitive data protection.
4) **Scalable and Cost-Effective Implementation**: Our system's architecture is designed for scalability, capable of processing thousands of transactions per second to accommodate the frequent updates required in supply chain operations. The use of Polygon's Layer 2 scaling solution significantly reduces transaction costs compared to Ethereum mainnet, making the system economically

viable for organizations of various sizes.

B. Security and Trust Framework

The security architecture of our system addresses multiple dimensions of trust that are essential in modern supply chains:

1) **Multi-layered Authentication**: The system implements robust authentication mechanisms through MetaMask integration, ensuring that only authorized participants can access and interact with the supply chain network. Each participant operates with appropriate access controls and functionality based on their role.
2) **Cryptographic Product Verification**: Our Dynamic & Encrypted QR code implementation provides a secure method for product authentication throughout the supply chain. By embedding encrypted payload information that can only be decrypted by authorized parties, we create a tamper-proof mechanism for verifying product authenticity.
3) **Smart Contract Governance**: The system deploys several interconnected smart contracts that manage different aspects of the supply chain, from product registration and ownership transfers to dispute resolution. These contracts execute automatically based on predefined conditions, reducing the need for intermediaries and minimizing the potential for disputes.
4) **Federated Security Intelligence**: The federated learning component not only preserves privacy but also enhances security by enabling the collaborative development of attack detection models. This allows the system to identify potential security threats and anomalies without exposing sensitive data, creating a collective defense mechanism against evolving threats.

C. Practical Implementation Considerations

While our system offers significant advantages, practical implementation requires careful consideration of several factors:

1) **Integration with Existing Systems**: Deploying blockchain and federated learning technologies in established supply chains requires thoughtful integration with legacy systems. Our implementation provides APIs and middleware components to facilitate this integration, but organizations must plan for transition periods and potential disruptions.
2) **Governance and Standards**: Effective implementation depends on establishing clear governance structures and standards for participation. This includes defining roles, responsibilities, data formats, and dispute resolution mechanisms. Our system provides the technical framework, but successful deployment requires organizational alignment among participants.
3) **Scalability Considerations**: While our system demonstrates good performance in testing environments, real-world deployment across global supply chains will present additional scalability challenges. Organizations should implement phased rollouts and continuous performance monitoring to ensure the system meets operational requirements.
4) **User Experience and Training**: The adoption of advanced technologies requires appropriate training and intuitive interfaces. Our system includes web-based interfaces designed for ease of use, but organizations should invest in training programs to ensure participants can effectively utilize the system's capabilities.

D. Comparative Advantages of Our Approach

Our integrated approach offers several advantages compared to traditional supply chain management systems:

1) **Comprehensive Data Security**: By combining blockchain's immutability with IPFS's content-addressing and federated learning's privacy preservation, our system provides end-to-end data security that exceeds what any single technology could offer. This comprehensive approach addresses the full spectrum of data security concerns in supply chains.
2) **Balanced Centralization-Decentralization**: While fully decentralized systems offer theoretical advantages, they often struggle with performance and governance issues. Our approach strikes a balance by using a permissioned blockchain with federated learning, providing the benefits of decentralization while maintaining practical governance and performance characteristics.
3) **Adaptive Intelligence**: The federated learning component enables the system to continuously improve based on collective experiences across the supply chain. This creates an adaptive intelligence layer that can evolve to address emerging challenges and opportunities without compromising data privacy.
4) **Cost-Effective Implementation**: Traditional supply chain technologies often require significant infrastructure investments. Our approach leverages existing computing resources through federated learning and minimizes blockchain transaction costs through Layer 2 scaling, making it more economically viable for a broader range of organizations.

While traditional identification technologies like RFID have played an important role in supply chain management, they face limitations in terms of security, cost, and infrastructure requirements. Our system addresses these limitations through its integrated approach, providing enhanced security, reduced infrastructure requirements, and improved cost-effectiveness.

VIII. Conclusion and Future Work

This work presents an enhanced supply chain management system integrating blockchain, IPFS, and federated learning. Key contributions include leveraging blockchain's immutable ledger and IPFS's decentralized storage for superior data integrity, transparency, and cost-effectiveness, while replacing RFID with dynamic, encrypted QR codes for improved security and accessibility. The system incorporates federated

learning for privacy-preserving collaborative intelligence, enabling anomaly detection without exposing sensitive data. This comprehensive approach provides a robust, scalable, and secure framework for product authentication, traceability, and combating counterfeiting, significantly advancing beyond traditional systems and prior blockchain implementations by addressing limitations in security, cost, and data management.

Future development will prioritize extending the system's capabilities to operate across multiple blockchain platforms. As blockchain adoption diversifies, achieving cross-chain interoperability is crucial for seamless integration within heterogeneous supply chain ecosystems involving various public and private ledgers. Research will focus on implementing mechanisms such as blockchain bridges or standardized interoperability protocols to enable secure and efficient asset transfers, data sharing, and smart contract interactions between different chains. This multi-chain expansion aims to enhance the system's flexibility, reach, and applicability in complex, global supply networks, ensuring wider compatibility and preventing vendor lock-in.

REFERENCES

[1] G. Narayanan, I. Cvitić, D. Peraković, and S. P. Raja, "Role of Blockchain Technology in Supplychain Management," in IEEE Access, vol. 12, pp. 19021-19023, 2024, doi: 10.1109/ACCESS.2024.3369190.

[2] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain," IEEE Access, vol. 5, pp. 17465-17477, 2017, doi: 10.1109/ACCESS.2017.2720760.

[3] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," in Proc. Int. Conf. Service Syst. Service Manage., Jun. 2017, pp. 1-6, doi: 10.1109/ICSSSM.2017.7996119.

[4] K. N. Hasan and K. Salah, "Proof of delivery of digital assets using blockchain and smart contracts," IEEE Access, vol. 6, pp. 65439-65448, 2018, doi: 10.1109/ACCESS.2018.2876971.

[5] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," Int. J. Prod. Res., vol. 57, no. 7, pp. 2117-2135, 2019, doi: 10.1080/00207543.2018.1533261.

[6] Oracle, "Blockchain for Supply Chain: Uses and Benefits," Oracle, Aug. 2024. [Online]. Available: https://www.oracle.com/blockchain/what-is-blockchain/blockchain-for-supply-chain/

[7] Deloitte, "Using blockchain to drive supply chain transparency," Deloitte, 2023. [Online]. Available: https://www2.deloitte.com/us/en/pages/operations/articles/blockchain-supply-chain-innovation.html

[8] ConsenSys, "Blockchain in Supply Chain Management," ConsenSys, 2024. [Online]. Available: https://consensys.io/blockchain-use-cases/supply-chain-management

[9] M. Tajima, "Strategic value of RFID in supply chain management," Journal of Purchasing and Supply Management, vol. 13, no. 4, pp. 261-273, 2007, doi: 10.1016/j.pursup.2007.11.001.

[10] A. Juels, "RFID security and privacy: A research survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381-394, 2006, doi: 10.1109/JSAC.2005.861395.

[11] S. E. Sarma, S. A. Weis, and D. W. Engels, "RFID systems and security and privacy implications," in Proc. Cryptographic Hardware and Embedded Systems, 2002, pp. 454-469, doi: 10.1007/3-540-36400-5_33.

[12] Y. Bendavid, E. Lefebvre, L. A. Lefebvre, and S. Fosso-Wamba, "Key performance indicators for the evaluation of RFID-enabled B-to-B e-commerce applications: The case of a five-layer supply chain," Information Systems and E-Business Management, vol. 7, no. 1, pp. 1-20, 2009, doi: 10.1007/s10257-008-0092-2.

[13] Lightspeed, "QR Code Inventory Management: A Comprehensive Guide," Lightspeed, Nov. 2024. [Online]. Available: https://www.lightspeedhq.com/blog/qr-codes-for-inventory-management/

[14] QR Code Chimp, "QR Codes for Supply Chain Management," QR Code Chimp, Sep. 2024. [Online]. Available: https://www.qrcodechimp.com/qr-codes-for-supply-chain-management/

[15] Scantrust, "Secure QR codes for anti-counterfeiting, with examples," Scantrust, 2024. [Online]. Available: https://www.scantrust.com/secure-qr-code-anti-counterfeiting-solutions/

[16] Acviss, "What is a Dynamic QR Code and Leveraging it for Brand Protection," Acviss, Jan. 2025. [Online]. Available: https://blog.acviss.com/what-is-dynamic-qr-code

[17] Filebase, "IPFS Storage Explained: How It Works," Filebase, Mar. 2025. [Online]. Available: https://filebase.com/blog/ipfs-storage-explained-how-it-works/

[18] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—Use cases, security benefits and challenges," in Proc. 15th Learning and Technology Conference, 2018, pp. 112-119, doi: 10.1109/LT.2018.8368494.

[19] Cloudflare, "Interplanetary File System (IPFS)," Cloudflare, 2024. [Online]. Available: https://developers.cloudflare.com/web3/ipfs-gateway/concepts/ipfs/

[20] G. Zheng, L. Kong, and A. Brintrup, "Federated machine learning for privacy preserving, collective supply chain risk prediction," International Journal of Production Research, vol. 61, no. 23, pp. 8115-8132, 2023, doi: 10.1080/00207543.2022.2164628.

[21] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," Journal of Information Security and Applications, vol. 50, 2020, doi: 10.1016/j.jisa.2019.102419.

[22] Medium, "Federated Learning: A Paradigm Shift in Data Privacy and Model Training," Medium, Mar. 2024. [Online]. Available: https://medium.com/@cloudhacks_/federated-learning-a-paradigm-shift-in-data-privacy-and-model-training-a41519c5fd7e