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

***Abstract*—Currently, counterfeit and stolen goods are a major concern for both online and traditional retailers. Consumers currently have no reliable way to confirm whether products are genuine, which erodes trust and results in financial losses for both purchasers and vendors. 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

Blockchain technology is revolutionizing various industries by offering a decentralized and immutable ledger that strengthens transparency and fosters trust. Its potential spans from securing financial transactions and boosting efficiency in banking [1], to safeguarding patient records in healthcare [2], and improving traceability in logistics [3]. Beyond these core domains, blockchain's versatility even extends to specialized use-cases: for example, Tran et al. [4] developed a decentralized system to filter spam calls in telecommunications, highlighting its broad applicability in strengthening security.

Supply chains, which have evolved into intricate global networks of manufacturers, distributors, and retailers, face growing challenges in product traceability and authenticity. Counterfeit goods inflict heavy financial losses on consumers and legitimate businesses, and pose serious health and safety risks in sectors such as pharmaceuticals, food, and electronics. Traditional supply chain systems—relying on centralized databases and barcodes—struggle with limited transparency, security vulnerabilities, and data-integrity issues. To overcome these hurdles, several blockchain-based architectures have been proposed: Tian [5] recorded HACCP data on a shared ledger to ensure secure, transparent food-safety tracking; Tajima [6] showed that automating RFID-based tracking with middleware and microchip tags improves visibility and reduces manual errors; Recent research by Narayanan et al. [7] demonstrated the potential of blockchain technology integrated with NFTs and RFID tags to create a secure product circulation system. Their approach utilized leveraging Non-Fungible Tokens (NFTs) as one-of-a-kind digital markers integrated with RFID tags and holographic labels to ensure product authenticity and traceability. While these approaches mark significant progress, they still face obstacles—RFID hardware remains expensive and specialized, and is vulnerable to security threats like cloning and eavesdropping, while storing full product metadata on-chain incurs substantial storage costs and can introduce privacy or security risks. Furthermore, consensus algorithms of some systems, while innovative, could be susceptible to security vulnerabilities such as Sybil attacks, where numerous fake nodes are created, and Bribery attacks aimed at compromising legitimate Primary Nodes (PNs).

To address these limitations, this paper proposes ChainFLIP—a novel framework that delivers significant advances in supply chain security and efficiency. Our major contributions are as follows:

1) We propose a novel blockchain-based framework for supply chain management, designed to enhance product authentication and traceability while reducing operational costs through dynamic encrypted QR codes and decentralized IPFS storage—overcoming limitations of traditional and prior blockchain models.
2) We introduce the integration of Federated Learning into the supply chain domain, enabling collaborative, privacy-preserving training of advanced security models to detect and mitigate threats like counterfeiting and fraud without exposing sensitive business data, thereby improving collective intelligence and resilience.
3) We perform extensive evaluations of the proposed system, assessing performance across key metrics such as security robustness, transaction throughput, storage efficiency, and cost-effectiveness. Results demonstrate superior scalability and efficiency compared to existing blockchain and traditional supply chain solutions.

Together, these contributions position ChainFLIP as a comprehensive, scalable framework ready to elevate security, transparency, and efficiency across modern supply chains.

TABLE I
COMPREHENSIVE COMPARISON OF SUPPLY CHAIN SYSTEMS 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.	✓	✓	✓	–	–	✓	–	–	–	✓

II. RELATED WORK

A. Blockchain Technology in Supply Chain Management

Blockchain technology offers transformative solutions for supply chain challenges. Toyoda et al. [8] introduced the Product Ownership Management System (POMS) integrating blockchain and RFID for post-supply authenticity verification, demonstrating feasibility on Ethereum. However, their focus was primarily on the post-supply chain phase, potentially limiting scalability in broader contexts. Tian et al. [5] integrated RFID with blockchain to develop a provenance-tracking system for agri-food supply chains in China, thereby markedly enhancing food safety oversight. However, because this solution was tailored specifically to the agri-food sector, it may lack the functionality required for broader application across other industries.

Hasan and Salah [9] introduced a smart-contract-driven proof-of-delivery framework built on a blockchain platform, designed to be customized for different courier services. While offering transparency, this approach lacked comprehensive product authentication mechanisms, and its complex contract structure could introduce scalability issues and higher transaction costs [7]. Saberi et al. [10] examined blockchain's role in promoting sustainable supply chains, emphasizing transparency and traceability. Their primary focus on sustainability, however, meant that critical security aspects and real-time tracking capabilities might have been overlooked.

Industry reports by Oracle [11] and Deloitte [12] highlight blockchain's ability to reduce administrative costs while improving transparency and transaction verification. ConsenSys [13] further emphasizes blockchain's role in enhancing cost-efficiency, consumer experience, and supply chain tradeability, although practical implementation challenges often remain.

B. RFID Technology and Limitations

RFID technology is widely used in supply chain management for real-time monitoring, error reduction, and improving efficiency [6]. However, as Tajima noted, it faces significant challenges such as high upfront implementation costs and the need for standardization across the supply chain. Hardware requirements for RFID readers create accessibility barriers for smaller participants, and critical security vulnerabilities like unauthorized reading, cloning, and data interception have been well-documented [14], [15]. Furthermore, the cost of item-level tagging often remains prohibitively high for widespread adoption [16].

Narayanan et al. [7] 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. While innovative, this dual-layered approach demands substantial additional infrastructure investment and complex system management, posing significant adoption challenges, particularly 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 [17] notes that encrypted QR codes restrict access to sensitive data, while QR Code Chimp [18] highlights their benefits in improving visibility, inventory tracking, and security. Secure QR solutions by Scantrust [19] and dynamic QR codes from Acviss [20] further enhance anti-counterfeiting measures by uniquely linking each item to real-time updates. While highly accessible and cost-effective, standard QR codes can be easily duplicated; thus, reliance solely on basic QR codes without robust encryption or dynamic features may not provide sufficient security against determined counterfeiters.

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. IPFS offers a decentralized alternative, providing efficiency through local caching and distributed storage [21], making it suitable for storing NFT metadata and decentralized applications. Research by Alketbi et al. [22] and Cloudflare [23] highlights that IPFS, combined with blockchain, ensures decentralized, cost-effective storage and data integrity via content-addressing.

Andara et al. [24] demonstrated a practical use of IPFS in a blockchain-based supply chain for traditional woven products in Indonesia, storing stage-wise documentation effectively. While showcasing feasibility and user benefits, the study also implicitly highlighted the latency trade-off inherent in decentralized storage systems like IPFS, which needs consideration during implementation.

E. Federated Learning for Privacy Preservation

Federated Learning (FL) enables multiple parties in the supply chain to collaboratively train fraud detection models without sharing raw data, ensuring privacy and compliance. Each node trains a local model and sends only updates for aggregation, allowing the global model to benefit from distributed knowledge [25].

Ferrag et al. [27] proposed FELIDS, a federated learning-based intrusion detection system for agricultural IoT infrastructures, demonstrating improved privacy and attack detection compared to centralized models. However, the direct applicability of such specialized systems to diverse and complex global supply chains might require significant adaptation.

Overall, while existing research demonstrates the significant potential of blockchain and related technologies in supply chain management, many approaches exhibit limitations regarding cost, scalability, security completeness, implementation complexity, or applicability restricted to specific sectors. This highlights the ongoing need for integrated, adaptable, and cost-effective solutions like the one proposed in this paper.

Table I provides a comprehensive comparison between our proposed system and other existing approaches, highlighting the key features and advancements. To enhance security and effectiveness, our system integrates robust aggregation techniques to filter out malicious updates and an incentive mechanism that rewards reliable participants. We adapt these federated learning advancements to supply chain environments, ensuring scalable, privacy-preserving collaboration among stakeholders.

III. Proposed System Architecture

A. Overall System Architecture

ChainFLIP consists of three core components—Dynamic & Encrypted QR codes for secure, on-demand product authentication; a decentralized storage system for scalable, tamper-proof metadata management; and Federated Learning for privacy-preserving threat detection and model updates.

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 some reference systems.
2) **Blockchain Layer**: Comprises the smart contracts deployed on a suitable blockchain network (e.g., a permissioned or public PoS network), handling product registration, ownership transfers, and dispute resolution.
3) **Storage Layer**: Utilizes a decentralized storage system (Blockchain & 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: 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. Table II provides a detailed comparison of our proposed system against the traditional approach and a reference system [7], highlighting key advancements across various parameters such as security, cost-efficiency, and traceability.

B. Blockchain Implementation

The blockchain layer ensures a secure, transparent, and immutable ledger for all product-related transactions. The system can be deployed on a public, Ethereum-compatible Layer 2 scaling solution offering high throughput and minimal fees, leveraging architectures designed for both scalability and decentralization. During development and testing, a public test network can be used to minimize risk, while a blockchain explorer provides comprehensive monitoring and on-chain verification of transactions and token metadata.

Such a blockchain platform brings several key benefits: it supports a high volume of transactions per second (*scalability*), minimizes operational costs via low gas fees (*cost-efficiency*), offers seamless integration with existing blockchain development tools, and secures the network through a distributed validator set. On-chain storage is optimized by recording product ownership, transaction history, decentralized storage content identifiers (CIDs), smart contract states, and dispute outcomes as lightweight references rather than embedding large datasets directly.

C. Smart Contract Design

Our system employs interconnected smart contracts, typically including:

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

These smart contracts interact seamlessly to create a comprehensive framework for managing the entire product lifecycle, from creation to final delivery. Deployment can be done using standard blockchain development tools and environments (e.g., web-based IDEs connected to the chosen network via browser wallets), allowing safe development and testing before mainnet deployment.

D. Dynamic and Encrypted QR Code Implementation

A key innovation in our system involves replacing traditional identification tags (like RFID) with Dynamic and

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

Parameter	Traditional System	Narayannan's System [7]	Our Proposed System
Traceability	Relies solely on conventional tracking methods	Reinforced by blockchain to guarantee full end-to-end traceability	Enhanced with blockchain and decentralized storage, 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	Offers limited visibility into the product lifecycle	Provides full transparency through immutable blockchain records	Full transparency with blockchain and decentralized storage records
Cost Efficiency	Incurs high expenses due to operational inefficiencies	Reduce costs with optimized consensus protocol and batch transaction processing	Reduced costs with efficient consensus, batching, data storage, and limited expensive physical equipment
Scalability	Faces significant limitations when scaling	Achieves better scalability by processing transactions in batches	Achieves better scalability by processing transactions in batches
Dispute Resolution	Resolves conflicts manually, often resulting in delays	Automates and clarifies dispute resolution via a transparent voting scheme	Automates and clarifies dispute resolution via a transparent voting scheme
Consensus Mechanism	Either unsupported or limited to basic consensus models	Customized consensus tailored for supply chain.	Customized supply chain consensus algorithms

Encrypted QR codes. This approach aims to provide enhanced security, greater accessibility, and improved cost-efficiency throughout the supply chain.

1) Multi-Layer Encryption Methodology: To secure product data, specifically the decentralized storage Content Identifiers (CIDs), we employ a multi-layer encryption strategy. The core of this is a *strong symmetric encryption algorithm* (e.g., AES-256 in CBC mode), which utilizes a robust key alongside random Initialization Vectors (IVs) for each encryption process. This use of unique IVs helps prevent pattern analysis, strengthening confidentiality. Complementing the encryption algorithm is rigorous *Key Management*, ensuring that encryption keys are stored securely with strict access controls to prevent unauthorized access. The structure of the encrypted payload is typically defined as:

EncryptedCID = IV + SymmetricEncrypt(CID, SecretKey)

2) Data Integrity Verification via HMAC: Ensuring data integrity during transmission and storage is crucial. For this, our system utilizes a *standard HMAC function* (e.g., using SHA-256). This cryptographic function generates a secure verification hash by combining the encrypted CID and a secret HMAC key. Before any attempt to decrypt the CID, this *Verification* step is performed; the received HMAC is compared against a recalculated HMAC. A mismatch indicates potential tampering, thus preventing the use of compromised data. The HMAC is computed as follows:

HMAC = HMAC_Function(EncryptedCID, HMACKey)

3) QR Code Generation and Usage: The generated QR code embeds the necessary components for secure data retrieval. The payload structure is typically:

QR Payload = IV : EncryptedCID : HMAC

Upon scanning the QR code, typically with a standard smartphone application, the embedded payload is extracted. The system first verifies the data's integrity using the included HMAC. If the verification is successful, the IV and the encrypted CID are used with the appropriate secret key to decrypt the original decentralized storage CID, allowing retrieval of the associated product information.

4) Advantages over Traditional Tags: Our dynamic and encrypted QR code system presents several advantages compared to traditional tags like RFID. Notably, it offers significantly *Lower Cost*, as QR codes can be easily printed on standard labels without requiring specialized, expensive tag hardware. This also contributes to *Greater Accessibility*, since codes can be scanned using ubiquitous smartphones, eliminating the need for dedicated readers. From a security perspective, the system provides *Stronger Security* through its integrated encryption and HMAC verification layers. Furthermore, the system supports *Dynamic Updates*; if product information changes, a new QR code reflecting the updated data can be generated and associated with the product. This combination of low cost and ease of use fosters *Inclusive Access*, making advanced supply chain tracking feasible for businesses of all sizes, not just large enterprises with significant hardware budgets.

IV. SECURITY MODELING WITH FEDERATED LEARNING

In the ChainFLIP system, Federated Learning (FL) serves as an intelligent security layer, focusing on detecting and preventing threats during the transaction batch proposal process. Each node in the network (including manufacturers, transporters, markets, and arbitrators) collects real-time transaction data from the blockchain via Polygonscan API. This process is performed by calling the API with parameters such as wallet address, start block, end block, and API key. The collected data includes features such as transaction value, gas consumption, gas price, sender/receiver addresses, and transaction logs. At each node, data is preprocessed, normalized using Standard-

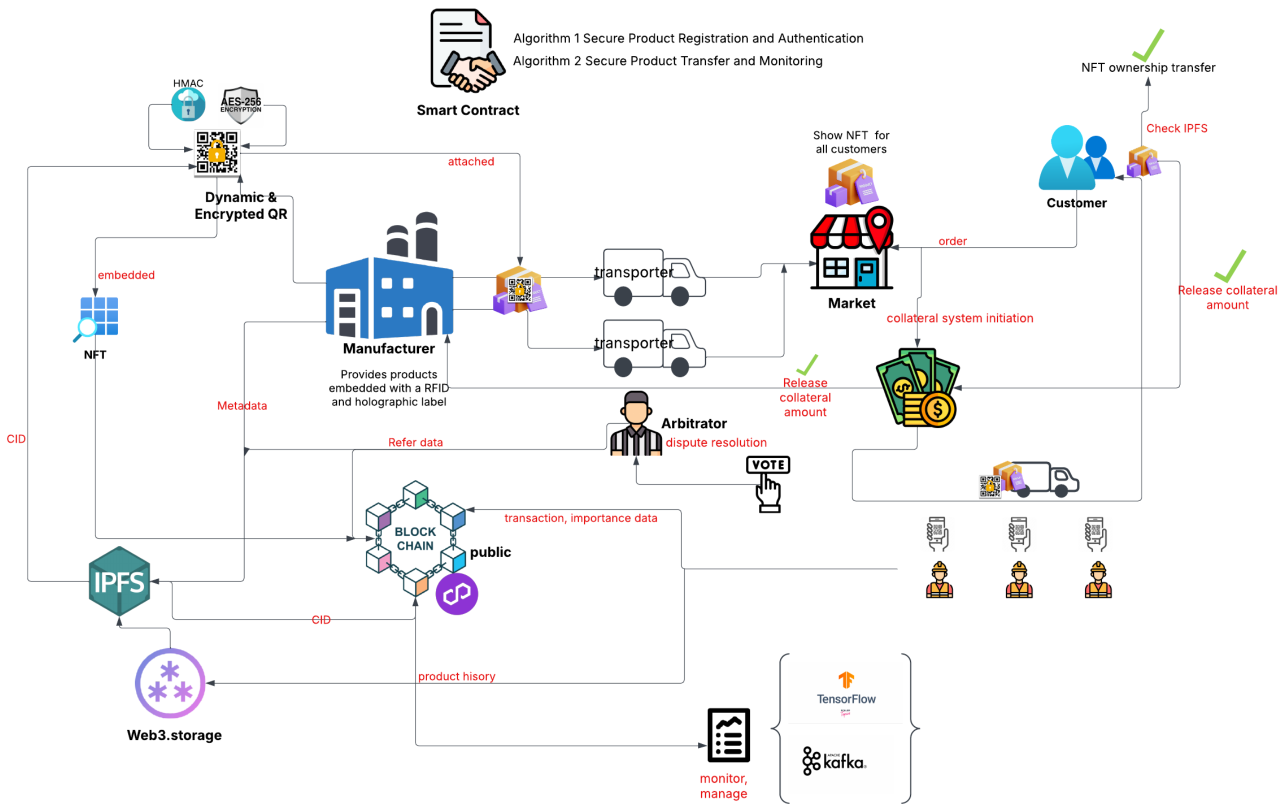

Fig. 1. Secure and Transparent System Workflow for Product Lifecycle Management

Scaler, and stored locally, ensuring no sensitive information is shared outside the organization.

Based on this local data, each node trains a simple neural network model (MLP with a hidden layer of 64 neurons and ReLU activation function) to detect anomalies and assess transaction risks. This model is built using TensorFlow with a Sequential structure, including an input layer that receives normalized features, a hidden layer with 64 neurons and ReLU activation, and an output layer with sigmoid activation for binary classification. During training, only model parameters (weights and gradients) are shared with the aggregation server through TensorFlow Federated, while the original data never leaves the node. The Federated Averaging (FedAvg) algorithm is used to aggregate updates from multiple nodes, creating a global model capable of effectively detecting fraudulent behaviors during the transaction batch proposal process.

FL is particularly effective in detecting and preventing Sybil and bribery attacks. We have identified security vulnerabilities in the Supply Chain Consensus (SCC) algorithm of Narayanan et al's system during the transaction batch proposal process, where Primary Nodes (PNs) acting as validators can be subject to Sybil and Bribery attacks. When attackers create multiple fake nodes and conduct small transactions to build reputation or exploit the random node selection process to increase their chances of entering the Primary Node pool—and eventually being selected as Validators—they may also bribe other Validators when counterfeit shipments are detected. The Federated Learning model can quickly identify abnormal transaction patterns and unauthorized payments between nodes. This process is performed by analyzing features such as transaction value and gas consumption, combined with node classification based on value threshold. When suspicious activities are detected, the system sends alerts and risk scores to the backend, which triggers smart contracts such as NodeManagement to isolate risky nodes and restrict their validation rights.

It's important to note that FL only participates in the transaction batch proposal process, not in the entire product lifecycle such as minting NFTs or disbursing payments. The FL training process is conducted over 10 rounds, each updating the global model and tracking accuracy. After training, the global model is used to assess the risk of transactions, classifying them as "high risk" or "low risk".

Incorporating Federated Learning into the ChainFLIP framework marks a significant step forward for blockchain-based supply chain security. This approach establishes a collaborative intelligence layer that maintains privacy while effectively detecting Sybil attacks and Bribery threats without exposing sensitive commercial data. This technological advancement enhances security, transparency and resilience across supply chain networks, supporting the fundamental values of decentralization, privacy protection, and trustworthy systems.

V. IMPLEMENTATION DETAILS

Our system is built on a robust technology stack designed for security, scalability, and decentralization. The blockchain component leverages the Polygon network, specifically the Mumbai Testnet during development and testing, chosen for its high throughput and low transaction costs. Smart contracts, which define the core business logic, are written in Solidity and managed within the Remix IDE environment. For decentralized storage of product metadata and associated files, we utilize the InterPlanetary File System (IPFS) through the Web3.Storage service, ensuring data persistence and integrity. The intelligence layer integrates TensorFlow Federated (TFF) for privacy-preserving federated learning, supporting tasks such as anomaly detection and reputation scoring, while maintaining data privacy. The user interface is developed using React.js, with blockchain interactions facilitated via ethers.js and MetaMask for wallet management. Product identification is achieved through dynamic and encrypted QR codes, generated and scanned using JavaScript libraries such as qrcode.react and react-qr-reader. Enhanced security is provided by cryptographic techniques like AES-256-CBC encryption and SHA-256-based HMAC for ensuring QR code data integrity, all managed using the Node.js crypto library.

Figure 1 presents the end-to-end ChainFLIP workflow and component interactions: product metadata is anchored on IPFS and linked via dynamic, encrypted QR codes to NFTs on Polygon; smart contracts manage node registration, trade lot proposals, dispute resolution, NFT transactions, escrowed and validated on-chain; and federated learning nodes continuously update security models.

The operational workflow begins with product registration, where the seller uploads product metadata to IPFS, generating a unique Content Identifier (CID), and simultaneously creates an encrypted QR code containing this CID for the physical product. Next, an NFT representing the product is minted on the Polygon blockchain, linking the product ID, the seller's account, and a hash of the IPFS CID. Any participant can later authenticate the product by scanning the QR code; the frontend verifies code integrity, decrypts the payload to retrieve the CID, fetches metadata from IPFS, and cross-references the IPFS data hash with the hash stored in the product's NFT on-chain. For sales, the owner lists the NFT on the Marketplace contract, initiating the transaction process. Buyers then deposit the required funds into the contract's secure escrow, which protects both parties by holding payment until conditions are met. The critical NFT transfer and subsequent fund release to the seller are triggered only after the buyer explicitly confirms physical receipt and successful product authentication against its immutable blockchain record. Should issues arise regarding authenticity or condition, the dedicated DisputeResolution contract provides a structured process for managing conflicts. Concurrently, network nodes engage in federated learning cycles. They collaboratively train models for tasks like anomaly detection or reputation scoring without exposing sensitive raw data, preserving privacy.

Several interconnected smart contracts govern the system's operations. The *SupplyChainNFT Contract*, based on the ERC721 standard, manages the lifecycle of product NFTs, including minting (restricted to authorized sellers, storing the IPFS hash), standard ownership transfers, and retrieval of transaction history. The *Marketplace Contract* facilitates the commercial aspects, handling product listings, escrow services

Algorithm 1 Secure Product Registration and Authentication

Input: Product Details (ID, batch, dates, type, etc.), Seller Account, Seller Reputation Score (from FL)
Output: NFT Token ID, Authentication Status

Phase 1: Product Registration (Seller)
Verify Seller Reputation Score $\geq$ Threshold$_{min_reputation}$
if Seller Reputation is insufficient **then**
    Return "Registration Failed: Seller reputation too low"
end if
Generate unique Product ID
Store detailed Product Metadata (specs, images) on IPFS, obtain CID
Encrypt CID using AES-256-CBC with unique IV
Generate HMAC for Encrypted CID + IV using SHA-256
Create QR Payload: IV : EncryptedCID : HMAC
Generate Dynamic & Encrypted QR Code from Payload
Mint NFT (ERC721) on Blockchain:
    Associate NFT with Product ID, Seller Account
    Store IPFS CID Hash (unencrypted) in NFT metadata
Attach physical QR Code to product
Return NFT Token ID
Phase 2: Product Authentication (Any User)
Scan QR Code from physical product
Extract IV, EncryptedCID, HMAC from QR Payload
Verify HMAC integrity using SHA-256 and stored HMACKey
if HMAC verification fails **then**
    Return "Authentication Failed: QR code integrity compromised"
end if
Decrypt EncryptedCID using AES-256-CBC, IV, and stored SecretKey to get original CID
Retrieve NFT data from Blockchain using Product ID or Token ID
Retrieve stored CID Hash from NFT metadata
Compute hash of the decrypted CID
if Hash of decrypted CID matches stored CID Hash **then**
    Retrieve current owner from NFT data
    Return "Product Authenticated: Owner is [Owner Address], Data CID is [CID]"
else
    Return "Authentication Failed: Product data mismatch (CID verification failed)"
end if

during purchases, and the final settlement involving NFT transfer and payment release upon buyer confirmation. It also logs transport details. The *DisputeResolution Contract* provides a framework for managing conflicts, allowing parties to raise disputes, submit evidence, and enabling designated arbitrators to resolve issues based on predefined rules. To optimize costs and network efficiency, the *BatchProcessing Contract* allows participants to bundle multiple actions, like registering several products or updating statuses, into a single blockchain transaction. Finally, the *NodeManagement Contract* oversees participant involvement, managing their registration, verification status, and reputation scores, which are crucial for the federated learning process and overall system.

Algorithm 2 Secure Product Transfer and Monitoring

Input: NFT Token ID, Seller Account, Buyer Account, Price, Seller Reputation, Buyer Reputation, Transaction Anomaly Score (from FL)

Output: Transfer Status

Phase: Secure Transfer and Sale (Seller, Buyer)
Verify Seller Reputation Score $\geq$ Threshold$_{min_reputation}$
Verify Buyer Reputation Score $\geq$ Threshold$_{min_reputation}$
if Seller or Buyer Reputation is insufficient **then**
    Return "Transfer Failed: Involved party reputation too low"
end if
Seller lists NFT for sale on Marketplace contract, setting Price
Buyer initiates purchase for NFT Token ID
Verify Buyer has sufficient funds
// FL Integration Point: Check Transaction Anomaly Score
if Transaction Anomaly Score $\geq$ Threshold$_{anomaly}$ **then**
    Flag transaction for review; potentially halt automated process
    Return "Transfer Halted: Potential anomaly detected"
end if
Buyer deposits collateral (e.g., purchase price) into Marketplace contract
// Ownership might transfer here conditionally based on contract logic
Seller (or Transporter) ships physical product to Buyer
Buyer receives product
Buyer performs Authentication (using steps from Algorithm 1, Phase 2)
if Authentication successful and product condition acceptable **then**
    Buyer confirms receipt via Marketplace contract
    Marketplace contract finalizes NFT ownership transfer to Buyer on Blockchain
    Marketplace contract releases payment from collateral to Seller
    Return "Sale and Transfer Completed Successfully"
else
    Buyer initiates dispute via DisputeResolution contract
    Return "Dispute Initiated: Authentication/Condition Issue"
end if

Our system's core functionality is driven by two primary algorithms that encapsulate the secure product lifecycle, integrating authentication, transfer, and monitoring enhanced by insights from federated learning.

The first algorithm details the secure registration process, where a product is linked to an NFT and an encrypted QR code pointing to its metadata on IPFS. It integrates a check on the seller's reputation, informed by federated learning, before allowing registration. It also outlines the comprehensive authentication procedure available to any user, involving QR code scanning, integrity verification via HMAC, decryption of the payload to retrieve the IPFS CID, and cross-validation against the data stored on the blockchain.

The second algorithm focuses on the secure transfer of product ownership during a sale. It incorporates checks derived from federated learning, such as verifying the reputation of both the buyer and seller and evaluating a transaction anomaly score to flag potentially suspicious activities before proceeding. The process culminates in the buyer authenticating the received product, followed by the smart contract finalizing the NFT ownership transfer and payment release.

VI. EXPERIMENTAL RESULTS

A. Supply Chain Consensus (SCC) Algorithm Evaluation

We evaluated the implemented Supply Chain Consensus (SCC) algorithm's performance through Hardhat tests on the Amoy test network, simulating batch proposal, validator selection, voting, and commitment based on a 66% supermajority threshold. The setup involved 5 Secondary Node (SN) proposing batches of ten transactions and 15 Primary Nodes (PNs) acting as potential validators, selected based on reputation.

Performance metrics revealed the operational characteristics on the testnet. The average batch proposal time was approximately 7.61 seconds with a gas cost of 582,199. Validation voting averaged 6.33 seconds and 65,522 gas per vote. Successfully committing a batch took about 8.81 seconds and cost 186,550 gas. Over the ten test runs, the success rate was 100%, and the measured throughput was low at 0.01 Transactions Per Second (TPS).

The reputation mechanism functioned correctly, adjusting scores based on participant actions: correct validators gained 40 points, incorrect validators lost 5 point, proposers of successful batches gained 25 points, and proposers of failed batches lost 10 points. While confirming the functional correctness of the SCC algorithm and its incentive structure, the observed latency and gas costs on the Amoy testnet suggest that further optimization or evaluation on alternative network infrastructures might be beneficial for high-volume applications.

B. Security Analysis

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.

Tamper Detection: We conducted tamper detection tests by deliberately modifying the encoded data in both systems. Based on analyses of typical RFID vulnerabilities found in security literature, standard RFID systems might detect tampering in approximately 85% of cases. In contrast, our Dynamic & Encrypted QR system achieved a 100% detection rate in simulations due to the integrated 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 two systems: the system proposed by Narayanan et al [7], and our proposed system. Since the original source code and specific implementation details for Narayanan et al. [7]'s system were unavailable, we reimplemented their proposed architecture based on the descriptions and algorithms presented in their paper for this comparative analysis. Therefore, the cost figures for their system presented in Table IV reflect our implementation and may differ from the original. Table IV summarizes the cost comparison. The analysis reveals that our proposed system incurs lower operational costs compared to our implementation of the system proposed by Narayanan [7] et al. This cost advantage stems primarily from key architectural differences, such as the elimination of dedicated reader hardware, reduced tag costs through the use of standard identifiers, and the strategic utilization of IPFS for partial data storage, which avoids the higher costs associated with storing all data directly on the blockchain. Furthermore, the modular design of our approach simplifies future upgrades and reduces maintenance overhead, potentially leading to additional cost savings over the system's lifecycle. Sensitivity analysis indicates that even under increased transaction volumes, our system maintains favorable cost-effectiveness due to its scalable infrastructure.

D. IPFS Performance Analysis

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

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.

TABLE III
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

E. Evaluating Federated Learning Effectiveness for Enhanced Security

To assess the effectiveness of the integrated federated learning (FL) component in strengthening system security against advanced attacks, we conducted experiments using simulated supply chain transaction data distributed across multiple nodes. The goal was to evaluate the FL-trained collaborative model's ability to detect not only general anomalies but also specific threats such as Sybil and Bribery attacks, while preserving local data privacy.

Each simulated node received a unique local dataset with features like transaction value (ETH), gas consumed, gas price (Gwei), and behavior labels (VALID/FRAUDULENT or NORMAL/SUSPICIOUS). Nodes trained local multi-layer perceptrons (using ReLU and sigmoid activations) to identify patterns such as rapid micro-transactions (Sybil) or unusual validator payments (Bribery). Only model updates (gradients or weights) were shared securely with a central server, which used the Federated Averaging (FedAvg) algorithm over ten rounds to build an enhanced global model capable of detecting these threats. Key outputs included the global model, risk scores for nodes/transactions, and standard ML metrics (accuracy, precision, recall, F1-score, convergence, fairness).

Using a real blockchain dataset split across five simulated nodes, the FL model achieved 96.5% average accuracy—nearly matching centralized training (97.5%) and outperforming isolated local models (85–90%). It reached over 95% precision and recall, with an F1-score of 0.96 in detecting suspicious behaviors. These results support a stronger decentralized reputation system informed by FL-driven insights.

The model converged efficiently, exceeding 95% accuracy within seven rounds, and showed fairness, with accuracy variance across nodes under 4%. When tested under non-IID data conditions, performance briefly dropped 2–4% but was recovered via clustered FL techniques. Overall, these findings validate FL's effectiveness for privacy-preserving, distributed threat detection in supply chains, with strong accuracy, robustness, and targeted defenses against Sybil and Bribery attacks.

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.

TABLE IV
COST ANALYSIS CONSIDERING DISTANCE IN MILES, GAS UNITS, AND COST REDUCTIONS

Distance (miles)	Number of Transporters	Narayanan et al [7]'s System		Our Proposed System Cost per Product		Cost Reduction (%)
		USD	Gas Units	USD	Gas Units	
50–100	1	0.022	3,200,000	0.020	2,900,000	9.1%
100–250	2	0.029	4,150,000	0.026	3,800,000	10.35%
250–500	3	0.037	5,310,000	0.033	4,832,000	10.8%
500–750	4	0.045	6,530,000	0.041	5,950,000	8.8%
750–1000	5	0.052	7,600,000	0.047	6,790,000	9.6%

A. System Implications and Contributions

The integration of blockchain technology, IPFS, and federated learning in our system introduces a comprehensive and transformative framework for supply chain management. One of the core contributions is enhanced data integrity and transparency. The immutable nature of blockchain ensures that every transaction is permanently recorded and resistant to tampering, allowing all authorized participants to independently verify the authenticity and history of products. This is further reinforced by IPFS, which identifies files based on their content rather than their location, offering an additional layer of data immutability and integrity.

Another key contribution is the decentralized architecture of the system, which distributes both data storage and processing across a peer-to-peer network. This eliminates single points of failure and enhances the overall resilience of the supply chain infrastructure, a critical requirement for global operations that demand high availability. The system also introduces privacy-preserving intelligence through federated learning, enabling participants to collaboratively train machine learning models without exposing raw data. This approach effectively balances the need for cross-organizational collaboration with the imperative of protecting sensitive business information.

The system achieves high cost-effectiveness by leveraging existing resources, using Layer 2 to reduce blockchain transaction fees, and employing IPFS for decentralized storage, cutting infrastructure and data management costs. Compared to RFID and traditional models, this solution offers superior security, scalability, and economic efficiency.

B. Security and Trust Framework

Our system is built upon a multi-layered security architecture designed to foster trust among supply chain participants. Authentication is enforced through MetaMask integration, ensuring that only authorized users can access and interact with the network. Each participant operates under clearly defined access controls aligned with their specific role in the supply chain. The use of dynamic and encrypted QR codes enhances product verification by embedding payloads that can only be decrypted by authorized entities, thereby providing a secure and tamper-proof mechanism for product authentication.

In addition, smart contracts govern critical functions such as product registration, ownership transfer, and dispute resolution. These contracts execute predefined logic autonomously, reducing reliance on intermediaries and minimizing the potential for conflicts. The inclusion of federated learning further strengthens the trust model by enabling the collaborative development of anomaly detection models across multiple participants without sharing sensitive data. This creates a decentralized, collective security intelligence that continuously evolves to detect and respond to emerging threats, while preserving data privacy.

C. Practical Implementation Considerations

Despite the system's benefits, practical deployment requires careful planning.Integrating blockchain and federated learning into supply chains requires compatibility with legacy systems. Our solution addresses this via dedicated APIs and middleware, but organizations should plan for transition time and challenges. Governance is crucial; clear standards for roles, data formats, and dispute resolution must be established. While our system offers the technical base, organizational coordination is vital for success. Scalability remains a concern-phased rollouts and ongoing performance monitoring are needed for global use. User experience is prioritized through intuitive web interfaces, but effective training is essential. Addressing these factors ensures smooth deployment and maximizes impact in real-world supply chains.

D. Comparative Advantages of Our Approach

Our integrated system architecture offers distinct advantages over traditional supply chain management technologies. It ensures comprehensive data security by combining blockchain's immutability, IPFS's content-based addressing, and federated learning's privacy-preserving capabilities—offering end-to-end protection that addresses both technical and governance concerns.

The system strikes a balance between decentralization and operational practicality. While fully decentralized models often suffer from governance and performance bottlenecks, our use of a permissioned blockchain and federated learning retains decentralization benefits without sacrificing control or efficiency. The adaptive nature of federated learning introduces an evolving intelligence layer, allowing the system to learn from shared, private insights and respond dynamically to new challenges.

Finally, the approach is cost-effective. It reduces infrastructure and data management costs by leveraging participants' existing resources and applying Layer 2 scaling to minimize blockchain fees. Compared to RFID, which requires expensive hardware and infrastructure, our solution delivers greater security, scalability, and affordability.

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 focus on enabling the system to operate seamlessly across multiple blockchain platforms. As blockchain adoption diversifies, cross-chain interoperability becomes essential for modern supply chain networks. We plan to research and implement solutions such as blockchain bridges and standardized interoperability protocols to support secure asset transfers and data sharing between heterogeneous ledgers. This would enhance system flexibility, prevent vendor lock-in, and support collaboration in complex, global supply chains.

References

[1] M. Author et al., "Blockchain in Finance: A Systematic Literature Review," *Preprint*, Jan. 2025. [Online]. Available: https://www.researchgate.net/publication/378223353...

[2] O. Attia, K. Khoufi, A. L. N. Guibene, and F. Kamoun, "Blockchain technology in healthcare: A systematic literature review," *Int J Med Inform*, vol. 164, p. 104791, Aug. 2022. doi: 10.1016/j.ijmedinf.2022.104791.

[3] A. Dolgui, S. Ivanov, A. Pavlov, B. Sokolov, and F. Werner, "Blockchain applications in supply chains, transport and logistics: a systematic review of the literature," *Int. J. Prod. Res.*, vol. 58, no. 7, pp. 2069-2081, 2020. doi: 10.1080/00207543.2019.1650976.

[4] T. D. Tran, N. A. Tai, T. T. Anh, P. T. Duy, and V. H. Pham, "Towards Transparent Spam Detection: Sentinel Call - A Distributed Ledger Solution for Call Filtering," in *Proceedings of the 2024 International Conference on Multimedia Analysis and Pattern Recognition (MAPR)*, 2024, pp. 1–6. doi: 10.1109/MAPR63514.2024.10660773.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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/

[12] 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

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

[14] 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.

[15] 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.

[16] 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.

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

[18] 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/

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

[20] 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

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

[22] 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.

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

[24] M. J. Andara, H. Wijayanto, N. Agitha, R. B. Huwae, D. Wiraguna, and M. Rahaman, "Blockchain-based Supply Chain Solution Using IPFS and QR Technology for Traditional Weave in West Nusa Tenggara," *Jurnal Infotel*, vol. 16, no. 4, pp. 740–757, Nov. 2024. doi: 10.20895/infotel.v16i3.1195.

[25] H. B. McMahan, E. Moore, D. Ramage, and H. Yishay, "Communication-Efficient Learning of Deep Networks from Decentralized Data," *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2017, pp. 1273–1282.

[26] 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.

[27] 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.

[28] 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