Secure Supply Chain Provenance via PUF-Anchored NFTs and 6G Edge Networks

Fiza Siyal, Antonella Guzzo, Fahed Alkhabbas, Domenico Sacca, and Giancarlo Fortino, *Fellow, IEEE*

Abstract

We propose a novel blockchain-based traceability system that uniquely combines Physical Unclonable Functions (PUFs) and Non-Fungible Tokens (NFTs) to establish secure, tamper-evident, and verifiable digital identities for physical products. Unlike conventional approaches that rely solely on serial numbers or barcodes, our system uses embedded PUFs to generate a physically unclonable ID for each item, ensuring hardware-level authenticity. This PUF ID is cryptographically linked to an NFT minted on a public blockchain, encapsulating metadata such as product origin, manufacturing details, and certification status. Associating NFTs and certifications with PUF-tagged products not only provides transparent provenance but also enables decentralised validation of compliance and ethical standards. This methodology is distinct in its integration of immutable physical identity with blockchain-based digital certification, offering a robust solution for enhancing transparency, combating counterfeiting, and fostering trust across global supply chains. Furthermore, employing Edge and emerging 6G networks, our framework can execute PUF challenge–response and preliminary NFT minting directly at edge nodes. This establishes a real-time, low-latency architecture that reduces network congestion and gas costs for secure and sustainable supply chains.

I. Introduction

Supply chain management encompasses a multifaceted network of interdependent processes, including the strategic procurement of raw materials, the conversion of these inputs into finished products, and the orchestration of their distribution to end users. Legacy supply chains frequently depend on heterogeneous, paper-centred documentation and segregated information silos, an architecture that produces opaque, end-to-end visibility and amplifies vulnerability to illicit counterfeiting [1], [2].

Blockchain (BC), characterised by its immutability, transparency, and enhanced security, presents a robust solution to supply chain issues. The BC is a decentralised network that operates on a consensus mechanism to implement changes. The consensus algorithms validate and authenticate transactions, ensuring that public ledgers stay synchronised and that only legitimate transactions are included in the BC. The decentralised architecture of the BC technology guarantees a transparent environment, providing stakeholders with real-time access to essential information about the status of goods. The immutable nature of data stored ensures integrity, since it cannot be modified or erased, therefore guaranteeing the precision and reliability of information along the whole supply chain [3]. As BC infrastructures evolve and unified metadata schemas are promulgated, NFTs are anticipated to underpin next-generation supply chain ecosystems. The use of NFTs enables provenance continuity across heterogeneous platforms. Also, it facilitates the utilisation of tokenised inventory as verifiable collateral in supply chain financing. This in turn fosters more transparent, resilient, and adaptive logistical networks [2], [4]. NFTs consist of an immutable transaction record, enabling other participants in a supply chain to readily verify the provenance of a product as well as the ownership. Data recorded via a smart contract on the BC is resistant to destruction without consent. Consequently, a safe data flow exists among many stakeholders, with a comprehensive transaction history recorded across several nodes of a BC, ensuring its security [5]. The ERC-721 is an extensively used nonfungible token standard for the production and monitoring of digital assets.

Falcone et al. [6] linked PUFs to supply chain management by embedding each product with a smart tag whose silicon-rooted PUF fingerprint serves as the device's private key and identity and then recording every supply chain event on a blockchain using that identity for authentication and provenance. At manufacture, a tag's public key derived on-demand from the PUF response is enrolled on the ledger alongside product data. At each subsequent step (raw materials sourcing, production, distribution, and consumer authentication), actors invoke an NFC-enabled protocol in which the PUF regenerates its private key to sign challenge–response messages, and those signatures are verified both by peers and via on-chain transactions. This coupling ensures that (1) each physical item carries an unclonable, hardware-rooted identifier; (2) no secret key ever resides in non-volatile

This work is part of the project titled "The Digital Transformation of Brands in the Fashion Sector: New Emerging Technologies for the Management of the Production and Distribution Network (Digital-Brand)". Project Number: F/240033/01-03/X49. The project is announced by Ministerial Decree 2 in August 2019—Intervention to support R&D projects in the application sectors "Intelligent Factory," "Agrifood," "Life Sciences," and "High Performance Computing."

Digital Object Identifier: 10.1109/MWC.2025.3634094
Date of Current Version: 27 March 2026
Date of Publication: 1 January 2026

Fiza Siyal (corresponding author), Antonella Guzzo, Domenico Sacca, and Giancarlo Fortino are with DIMES, University of Calabria, 87036 Rende, Italy; Fahed Alkhabbas is with the Department of Computer Science and Media Technology, Sustainable Digitalisation Research Centre, Malmö University, 205 06 Malmö, Sweden.

memory; and (3) every transfer, location update, or certificate issuance is immutably anchored to that PUF-derived identity, enabling complete traceability and tamper evidence in a decentralised, high-integrity supply-chain framework.

We have proposed a novel framework that integrates physically unclonable functions (PUFs) with non-fungible tokens (NFTs) to deliver complete traceability and compliance assurance in complex supply chains. In this architecture, each product is embedded with a unique PUF that generates a hardware-rooted identifier, which is linked on-chain to an ERC-721 token containing detailed manufacturing metadata and ownership provenance. Legitimate certifiers with designated roles on the BC provide quality assessment of the product and attach a certificate of authenticity in the NFTs' metadata. During the transit of a product, every ownership transfer, inspection, and certification update is recorded on the digital ledger, leading to a tamper-proof trace of its entire lifecycle. This links an unclonable physical identity with digital attestation on BC results in a transparent and secure system. Our proposed architecture offers both the authenticity and certified status of each item at any point in its lifecycle.

Considering our proposed supply chain traceability architecture that incorporates PUF and NFT, we formulated the following research questions for further analysis.

- How accurately does this PUF-NFT-anchored proof of concept reflect real-world integration that includes an off-chain PUF reader simulation and a smart contract prototype?
- How well do the smart contract's role-based permissions (manufacturer, distributor, retailer, certifier) combined with the Elliptic Curve Digital Signature Algorithm (ECDSA) signature verification enforce that only authorised parties can register products, update locations, and issue certificates?
- What are the gas consumption and transaction latency profiles for PUF registration, product addition, NFT minting, and certificate issuance under controlled local BC settings?

A. Edge AI and 6G Networks for PUF-Anchored NFTs in Supply Chains

Advanced technologies like Edge AI and 6G networks complement to a greater extent our proposed architecture for Industry 5.0 supply chain systems [7]. For instance, ultra-low-latency links and pervasive edge servers offered by the 6G network enable local execution of the PUF challenge–response protocol, and responses are hashed and preliminarily verified without incurring the round-trip delays of a centralised server or public blockchain.

Further, by offloading NFT minting and certificate verification to edge nodes, transactions can be batched, pre-validated, and relayed in optimised blocks over dedicated 6G slices. This will reduce backhaul congestion with less gas consumption and transform into continuous service quality for supply chain operations.

Moreover, 6G's support for massive machine-type communication (mMTC) and sufficient device density allows every physical item, each equipped with its own PUF tag and low-power wireless interface, to be uniquely identified and authenticated for large deployments, without overwhelming core network resources.

In addition, implementing AI analytics at edge nodes facilitates consistent reporting of PUF signatures and supply chain operations and detection of anomalies (e.g., replay attacks, tampered sensors, counterfeit products, etc.), which results in early warnings and actions to stop conceivably fake or invalid NFT certificates from being released on the BC. Further, TinyML-based AI models can be deployed at edge nodes with administrative authority to detect compromised certifier nodes. The TinyML model learns patterns of normal transactions to identify irregular, inconsistent patterns in validation frequency, signing behaviour, or mismatched device identifiers that might indicate compromise.

Overall, the paper is arranged as follows: Existing relevant literature on supply chain traceability using blockchain NFTs and PUFs is discussed in Section II; in Section III, the proposed framework is presented; Section IV discusses experimental setup and analysis of results. Section V provides the threat security analysis of our proposed framework. Section VI compares our work with similar state-of-the-art approaches. The study is concluded in Section VII with limitations and possible directions for future work.

B. Motivation and Contributions

Conventional supply chains are composed of multiple independent actors, which complicates the maintenance of comprehensive provenance records and heightens vulnerability to counterfeit goods and manual data manipulation. Traditional tracking methods, including barcodes and RFIDs, are highly vulnerable to threats because of weak features inherent in tag construction. Therefore, these traditional tags can be easily cloned and altered, which introduces low traceability and transparency in existing supply chains. To overcome this, we propose a novel framework, which combines NFTs and PUFs to establish a secure supply chain system. In the framework, each product is associated with a unique, unclonable PUF identifier, which captures product metadata and ownership transfers as the product moves through the supply chain. This physical identity is further linked to an NFT on the BC. The NFT attaches a compliance certificate with PUF ID to represent proof of authenticity of that product and serve as a digital twin of the product. The convergence of PUF and NFT establishes a strong protection mechanism at both the physical and digital levels. The framework guarantees robust traceability and tamper-evident provenance of the product. The significant contributions are outlined as follows:

- We proposed a novel architecture that combines PUFs with NFTs. This framework establishes hardware-anchored digital twins that bind each product's unique PUF identifier to an on-chain NFT token ID for robust provenance and immutable mapping between the physical item and its digital record.
- Developed a proof-of-concept deployment, with off-chain PUF reader simulation using pypuf and ECDSA modules in Python, JSON-driven signature workflows, and a smart contract to validate the feasibility and correctness of the PUF-NFT anchored product lifecycle.
- Extended OpenZeppelin's ERC-721 and Access-Control modules to enforce fine-grained permissions and integrate Ethereum-standard ECDSA message signing over (pufId, challenge), ensuring

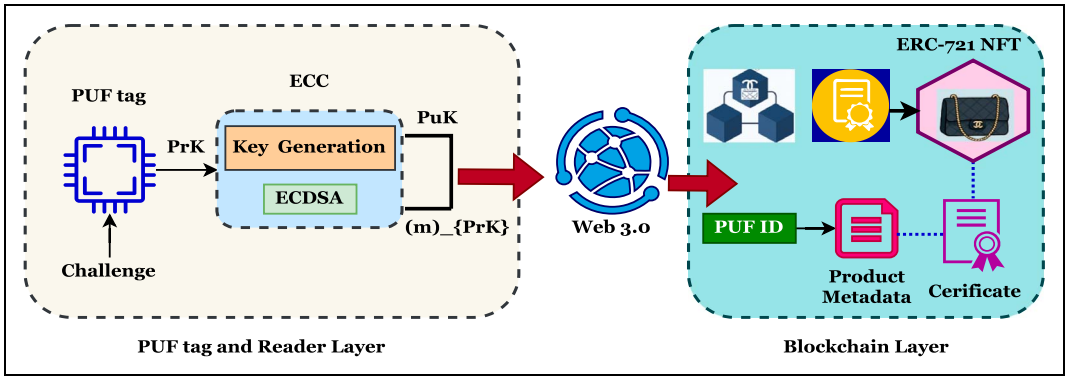


FIG. 1. PUF-Anchored NFT Framework for supply chain security. The PUF tag and reader layer transform a hardware challenge-response into an ECC private key, whose derived public key and ECDSA signature are sent via a Web3 gateway. The blockchain layer implements a smart contract that mints an ERC-721 NFT. The NFT links to product metadata and certificate records.

only legitimate stakeholders can register products and issue authenticity certificates.

- Through systematic benchmarking, we quantify gas costs for PUF registration, product addition, NFT minting, and certificate issuance, and analyse latency under realistic transactions to forecast the overall cost of the luxury product supply chain.

II. Related Work

Recent studies explored NFTs in relation with traceability, authenticity, and transparency for Industry 5.0 applications, in particular supply chains. Narayanan et al. [3] employed ERC-721 NFTs to capture product metadata such as origin, ownership, and authentication attributes, with RFID and holographic tags to strengthen provenance tracking and automate supply chain processes. In manufacturing, Habtemichael et al. [5] exploit NFTs to link digital twins with value-added metadata captured during product transit for traceability and transparency. Kumar et al. [8] use NFTs to register pharmaceutical products, to verify ownership and to automate compliance tracking via smart contracts. Ahuja et al. [9] designed SeedChain, where NFTs represent digital certificates of authenticity for seed batches. Smart contracts implement ownership and logistics functions, and off-chain storage IPFS is used to store product metadata for offloading BC storage. Usman et al. [10] present DSCoT, a cyber physical systems (CPS) framework based on NFT, which employed customised ERC-721 tokens to store identity, role, and access metadata for IoT devices, fog nodes, and users, enabling careful asset authentication and secure CPS interactions in smart city infrastructures. These studies collectively demonstrate how NFT metadata serves domain-specific functions ranging from regulatory compliance and lifecycle tracking to environmental monitoring and decentralised identity.

In the agricultural sector, Wang et al. [11] present a BC-based traceability framework for the cotton lint supply chain. The framework utilises non-fungible tokens (NFTs), which hold digital twins of physical products and confirm the authenticity of a product with a compliance certificate. Helo et al. [12] propose the use of NFTs in pharmaceuticals, manufacturing, and supply chains for provenance tracking, with emphasis on enhancing reliability and mitigating the risks of counterfeit or expired products.

ICtoken by Balla et al. [13] implements hardware IP protection by minting a unique NFT for each integrated circuit on a permissioned BC (ICtracker), encoding cryptographic hashes of the IC identifier, package markings, and encrypted active-metering data, while tracking ownership, PCB/device integration, and provenance with minimal on-chain storage. Hawashin et al. [14] extend this paradigm to UAV manufacturing, using self-sovereign identities to mint component NFTs linked to IPFS-stored digital twins, bundling identical parts into lot NFTs, and enabling manufacturers to redeem these lots for assembly under a management smart contract that enforces role-based minting, listings, and security controls, with off-chain metadata reducing gas costs. Davies et al. [4] further argue that NFTs' provable scarcity and ownership can underpin "phygital" certifications of product origin, emissions, and labour practices; a "mint-to-order" model that issues NFTs upon purchase and triggers production only on redemption to mitigate overproduction; and gamified incentives with fractional royalties to align stakeholder interests, contingent on interoperable standards and behavioural research for scalable, transparent, and sustainable supply chains.

These studies demonstrate that NFT metadata serves domain-specific functions ranging from regulatory compliance and lifecycle tracking to environmental monitoring and decentralised identity.

III. Proposed Framework

The BC framework in Fig. 1 presents a secure, verifiable method for product authentication and traceability by integrating PUFs, ECDSA-based digital signatures, and NFT-backed certification. In particular, it is highly suitable to address counterfeiting problems in fashion supply chains, where NFT plays the role of an immutable digital twin for each item on-chain. Initially, a PUF response inherently linked to the product's physical characteristics serves as a source for generating an ECC key pair. The private key is protected within the device or held by the issuing authority, while the corresponding public key is dedicated for authentication purposes.

The conceptual architecture of the proposed framework combines PUF-enabled authentication with BC-powered NFT provenance. Initially the PUF tag and reader layer with challenge and response generate a unique physical key (PrK) that is an integral part of device identity. Employing Elliptic Curve

Cryptography (ECC) and ECDSA, the corresponding private key (PrK) and public key (PuK) are obtained to create a signed message (m)_PrK. Next, this verified identity is communicated to the BC layer via the Web 3.0 interface, which registers this unique PUF ID with its relevant product metadata. Upon registration, a non-fungible token (NFT) is minted that links a digital certificate to the product's PUF ID, which serves as proof of authentication. This connection of digital certificate to PUF ID creates a secure cryptographic link of each item to its physical origin. The proposed design offers a tamper-evident connection between the physical product and its digital twin.

The smart contract inherits OpenZeppelin's AccessControl module, which enforces strict role-based permissions and prevents any compromised node from validating or signing new transactions. In the rare event of a certifier's private key being compromised, the manufacturer can immediately revoke the certifier's authorisation through the revokeRole() function integrated within the AccessControl framework. This mechanism ensures that affected entities are promptly isolated, eliminating the risk of unauthorised validations. Following that, a new certifier can be registered with a distinct key pair to maintain the integrity of the authentication process without disrupting system operations. In case of abnormal behaviour, the administrator (e.g., manufacturer) can invoke the revokeRole() function to instantly halt the certifier's access. The RevokeRole() function is not yet implemented in the current version. However, the algorithm for revokeRole() is presented in Algorithm 1.

Algorithm 1 Certifier Revocation Procedure

Begin
The manufacturer detects compromised certifier node C_{addr}
if $C_{addr} \in$ ActiveCertifiers **then**
    RevokeRole(CERTIFIER_ROLE, C_{addr})
    Record event $\langle C_{addr}, M_{addr}, timestamp \rangle$ in blockchain logs
    Update $CertifierStatus[C_{addr}] \leftarrow$ "Revoked"
else
    Reject request with message "Certifier not active"
end if
End

A. Logical Flow of Smart Contract From Signing a Message to Minting a Product

Fig. 2, the sequence diagram, illustrates the workflow of PUF-based product registration and NFT minting. Initially, the reader sends a random challenge to the PUF tag to verify its authenticity. This challenge is a one-time random value that acts as a nonce. The PUF generates a unique response based on its manufacturing randomness. The reader calculates two hashes based on the received PUF response:

1) responseHash = keccak256(pufResponse), used to validate authenticity later.
2) innerHash = keccak256(pufId, challenge), links the PUF ID with its issued challenge for message integrity.

Next, the signer or reader creates an Ethereum signed message (eth message) from the innerHash. This signature, coupled with the challenge and PUF ID, is transmitted to the smart contract. The function call is made to the smart contract, including all verification data. The contract performs two validation checks:

1) require(validPufIds[pufId] == responseHash), which verifies that the provided PUF response and the pre-enrolled valid PUF hash are the same.
2) recovered = ECDSA. recover(ethMsg, signature) and require(recovered == ethAddress) confirm that the sign comes from an authorised and legitimate user (e.g., the manufacturer).

For the valid signature, the contract stores the product record on-chain (including PUF ID, owner, timestamp, and location). As the product is added, an NFT corresponding to it is minted, which links metadata such as the PUF ID and certificate data into the token. For the invalid signature, the transaction is reverted using Revert("Invalid PUF or Signature"). This means no product record or NFT is created.

1) Authentication Protocol: Each authentication session begins with the verifier generating a random challenge nonce, ensuring that no two sessions reuse the same input. The PUF module computes the response only after receiving this nonce, binding the generated output to that session. Because the challenge and corresponding response are both time-stamped and verified on-chain, any attempt to replay an earlier transaction is automatically rejected, guaranteeing freshness and resistance against replay attacks.

2) NFT Metadata Management: To protect sensitive production information, one option is to encrypt the product metadata before uploading to off-chain storage such as IPFS. Authorised nodes can decrypt this data using shared keys managed through access-controlled registries. Another option is to implement a selective disclosure mechanism where only specific fields of data are disclosed, and other sensitive information is kept confidential. Also, zero-knowledge proof (ZKP) protocols can be employed to allow a participant to verify compliance without exposing the actual certificate content.

IV. Experiments and Results

A. Experimental Setup

We carried out all on-chain performance and cost measurements in a controlled Hardhat environment, compiling our SupplyChainNFT contract with Solidity v0.8.28 (optimiser enabled at 200 runs and viaIR turned on) to mirror realistic production settings. Deployment and interactions, covering PUF registration (addValidPufId), product addition and NFT minting (addProduct), certificate issuance (issueCertificateByToken), and signature verification, were executed against a localhost Hardhat node to ensure fast, deterministic block times. We leveraged the @nomicfoundation/hardhat-toolbox for Ethers.js support, hardhat-gas-reporter (configured to report gas consumption and timing details) to capture both monetary and time metrics for each transaction, and hardhat-contract-sizer running on every compile, focused on the SupplyChainNFT smart contract to monitor bytecode size. The code for this project is made available at this link: https://github.com/Fiza-Sial/PUF-anchored-NFT.

B. Results

Fig. 3 presents all eight unit tests for **SupplyChainNFT** passed on a local Hardhat network, confirming that role-based permissions, PUF-challenge verification, minting constraints, location updates, ownership

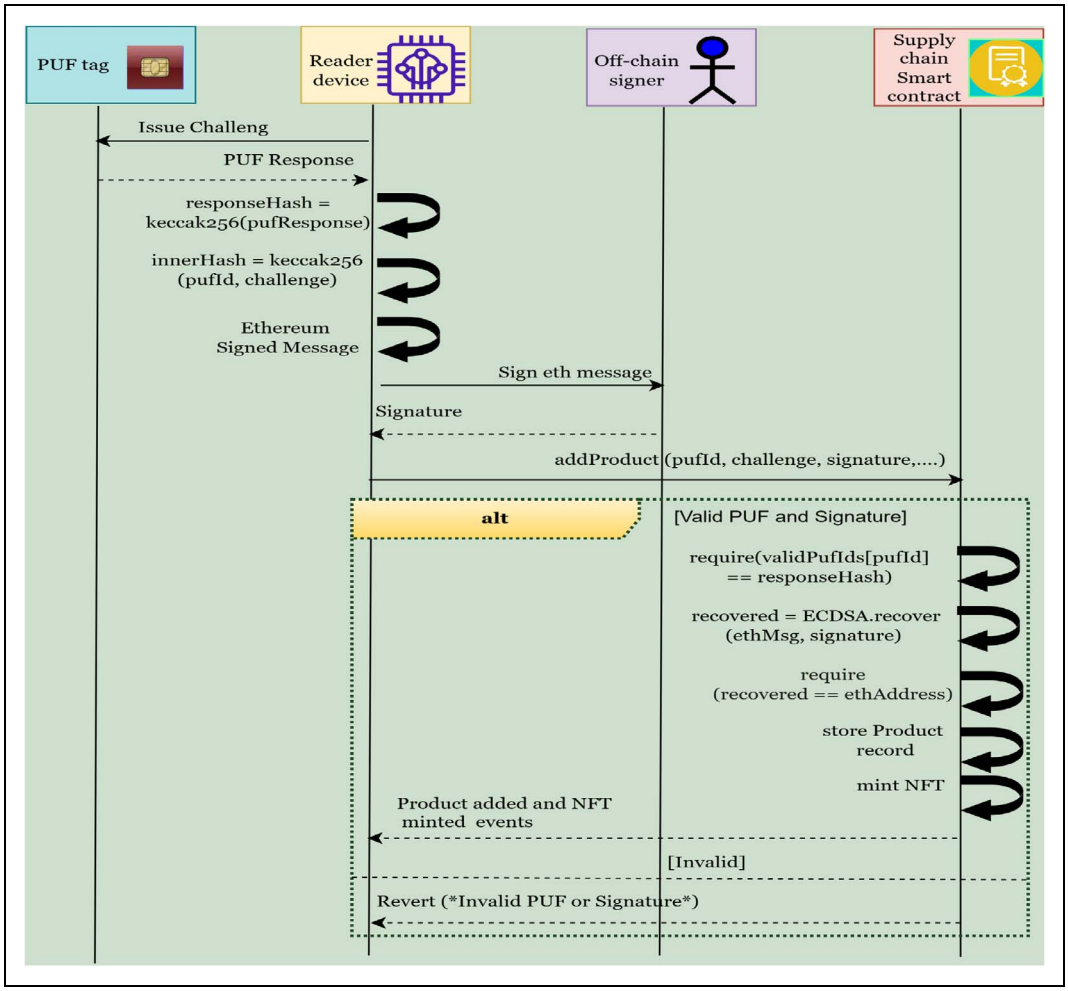


FIG. 2. Sequence diagram outlining the steps of PUF-based product registration and NFT minting.

transfers, and certificate issuance all behave correctly and securely under valid and invalid conditions. The tests demonstrate that only the manufacturer role can register PUF IDs and mint products; invalid signatures or double-mints are properly reverted; distributors and retailers can update locations with a valid off-chain PUF signature; only the current tag owner can transfer ownership via authenticated signature; and only certifiers can issue and retrieve certificates. Gas profiling across these tests also aligns with earlier benchmarks: **addProduct** is the most expensive at approximately ≈ 385 k gas because it both registers a new PUF ID, verifies off-chain signatures, writes multiple storage slots (including the ERC-721 mint and **tokenURI**), and emits events—while **issueCertificateByToken** follows at ≈ 119 k gas, **transferProductOwnership** at ≈ 84 k gas, **updateLocation** at ≈ 57 k gas, and **addValidPufId** is the cheapest at ≈ 47 k gas.

The results presented in Fig. 4(A) and 4(B) provide a comparison of gas consumption, latency and transaction cost for key operations in the proposed smart contract. As shown in the table, the addProduct function incurs the highest gas usage (433,013 units, ≈ $41.57), reflecting its complex logic. It performs multiple writes of state variables, involving registering the product, linking the PUF ID, minting the NFT and linking to PUF metadata. The latency trend in the same plot further confirms that addProduct with higher computational complexity corresponds to slightly increased transaction time with latency (101 ms). In contrast, issueCert remains moderately expensive in gas usage (164,025 units) with less latency variation (93 ms).

The simulation script orchestrates a test of our PUF-backed supply chain NFT workflow on a local Ethereum node with 5-second block times, programmatically loading a list of tag identities (PUF IDs paired with ECC keys, challenges, and hashes) and instantiating four role-based wallets (manufacturer, distributor, retailer, and certifier). For each tag, it mints an ERC-721 token tied to the PUF, immediately issues an initial on-chain certificate, then simulates two successive location-update "hops" (each signed by the tag's private key and submitted by the distributor and retailer). The smart contract performs a tag-authorised ownership transfer and finally issues a closing certificate. At each step it captures both gas usage and latency before aggregating all metrics into a results file.

The bar chart and accompanying cost table make it clear that the heaviest on-chain work happens when you register and mint a new PUF-backed product (**addProduct**), which averaged about 433 k gas (≈ $21.21), followed by issuing the first certificate (**issueCert**) at roughly 164 k gas (≈ $8.03). All of the **updateLoc** hops (64 – 69)k gas ≈ $3.18–$3.36), the ownership transfer (≈ 69 k gas, $3.40), and even the initial PUF registration (**addValidPufId** at ≈ 47 k

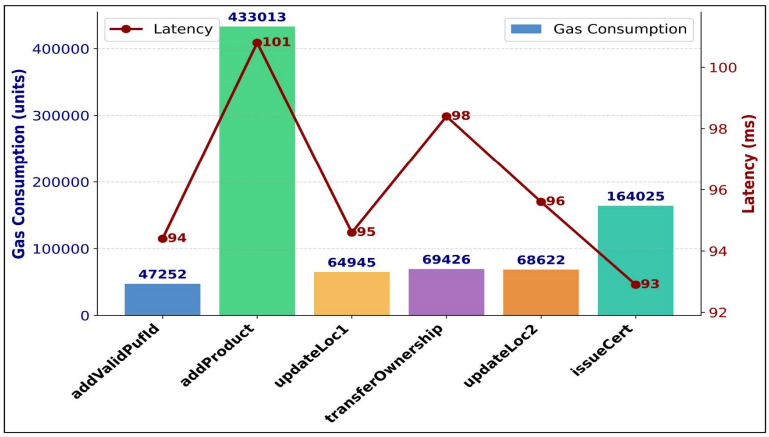
```
Fiza@Fiza-Siyal MINGW64 ~/nft (PUF)
$ npx hardhat test --network localhost
·----------------------|------------------------------|------------------------------·
|  Solc version: 0.8.28  ·  Optimizer enabled: false  ·  Runs: 200                    |
·----------------------|------------------------------|------------------------------·
|  Contract Name         ·  Deployed size (KiB) (change)  ·  Initcode size (KiB) (change)  |
·----------------------|------------------------------|------------------------------·
|  SupplyChainNFT        ·              19.496 (0.000)  ·              21.267 (0.000)  |
·----------------------|------------------------------|------------------------------·

  SupplyChain Traceability using PUF and NFT
    √ assigns roles properly (70ms, 385224 gas)
    √ reverts when non-manufacturer adds PUF ID (14ms, 410420 gas)
    √ verifies raw PUF hash correctly (4ms, 25196 gas)
    √ reverts on addProduct with invalid signature (50ms, 111743 gas)
    √ reverts on double mint (addProduct twice) (16ms, 73332 gas)
    √ allows authorized roles to update location with proof and reverts invalid proof or role (68ms, 160170 gas)
    √ transfers ownership and NFT with proof (89ms, 168376 gas)
    √ issues and retrieves certificate by token and reverts invalid role (45ms, 229717 gas)

·-----------------------------------------|---------------------------|-------------|-----------------------------·
|            Solc version: 0.8.28         ·  Optimizer enabled: false  ·  Runs: 200  ·  Block limit: 6718946 gas  |
·-----------------------------------------|---------------------------|-------------|-----------------------------·
|  Methods                                                                                                        |
·------------------|----------------------|-------------|-------------|-------------|--------------|--------------·
|  Contract        ·  Method              ·  Min        ·  Max        ·  Avg        ·  # calls     ·  usd (avg)  |
·------------------|----------------------|-------------|-------------|-------------|--------------|--------------·
|  SupplyChainNFT  ·  addProduct          ·          -  ·          -  ·     385224  ·           2  ·          -  |
·------------------|----------------------|-------------|-------------|-------------|--------------|--------------·
|  SupplyChainNFT  ·  addValidPufId       ·          -  ·          -  ·      47076  ·           1  ·          -  |
·------------------|----------------------|-------------|-------------|-------------|--------------|--------------·
|  SupplyChainNFT  ·  issueCertificateByToken  ·      -  ·          -  ·     119335  ·           1  ·          -  |
·------------------|----------------------|-------------|-------------|-------------|--------------|--------------·
|  SupplyChainNFT  ·  transferProductOwnership  ·     -  ·          -  ·      84262  ·           2  ·          -  |
·------------------|----------------------|-------------|-------------|-------------|--------------|--------------·
|  SupplyChainNFT  ·  updateLocation      ·          -  ·          -  ·      57283  ·           2  ·          -  |
·------------------|----------------------|-------------|-------------|-------------|--------------|--------------·

  8 passing (4s)
```

FIG. 3. Unit-Test outcomes and performance profiling (gas consumption and execution timings) of SupplyChainNFT smart contract.



A

Operation	Gas Units	Gas Cost (USD)
addValidPufId	47,252	$4.54
addProduct	433,013	$41.57
updateLoc1	64,945	$6.23
transferOwnership	69,426	$6.66
updateLoc2	68,622	$6.59
issueCert	164,025	$15.75

B

FIG. 4. (A) Gas Consumption and Latency analysis of core smart contract functions, (B) Gas Cost in USD.

gas, $2.31) are substantially cheaper. The observed distribution of gas costs aligns with the EVM's gas model: operations that initialise new state and perform extensive storage writes, namely, registering and minting a product and issuing its first certificate, incur the highest gas consumption, whereas subsequent location updates and ownership transfers simply modify existing mappings and therefore require significantly less gas. Quantitatively, the complete product lifecycle (minting + two updates + transfer + two certifications) averages approximately $30–$35 in total gas fees, with the bulk of that expenditure concentrated in the minting and initial certification steps. These measurements were obtained under controlled settings on a local Hardhat blockchain; actual gas usage and costs may vary slightly or even moderately when running on an Ethereum testnet or the mainnet.

Threat	Description	Mitigation	Outcome
MitM or Relay attack	Intercepts or alters messages between nodes.	ECC-based mutual authentication; invalid keys rejected.	Ensures entity authenticity and prevents message injection.
Replay Attack	Reuse of a valid challenge–response pair.	Random nonce and timestamp per session; old pairs invalidated.	Guarantees freshness and thwarts replay attempts.
Counterfeit Token	Forged NFTs or duplicated identifiers.	Each NFT bound to verified on-chain PUF ID; mismatched hashes rejected.	Prevents counterfeit entries and enforces unique identity binding.
Data Tampering	Modification of metadata or records.	Records hashed and anchored on blockchain ledger.	Preserves immutability and data integrity.
Key Compromise/Leakage	Exposure of certifier key or credentials.	Role-based access control with 'revokeRole()' recovery.	Limits breach impact and maintains trust continuity.
Rogue Smart Contract	Invocation of Contract functions by an attacker.	Role-based access control with authorised nodes.	Limits unauthorised access and function invocation.

TABLE I. Threat modeling and mitigation strategies.

Ref.	Main Focus	Blockchain	NFT-Based	PUF-Based	Supply Chain
[3]	Counterfeiting	Private	Yes	No	General
[5]	Traceability	Not specific	Yes	No	Manufacturing
[8]	Counterfeiting	Ethereum Testnet	Yes	No	Healthcare
[9]	Traceability, Transparency, Counterfeiting	Ethereum	Yes	No	Seed
[10]	Security & Authentication	Goerli Testnet	Yes	No	Smart Cities
[13]	Counterfeit, Traceability	Consortium, Permissioned	Yes	Yes	Hardware
[14]	Traceability	Ethereum	Yes	No	Manufacturing
This work	Traceability, Transparency, Counterfeiting	Ethereum	Yes	Yes	Luxury

TABLE II. Comparison with related studies.

V. Threat Modeling and Mitigation Strategies

To evaluate the robustness of the proposed framework, we conducted a threat analysis, focusing on common attack vectors relevant to blockchain-based authentication and traceability. The objective was to identify potential vulnerabilities that could undermine product provenance or disrupt communication among supply-chain participants and to map each risk to an appropriate mitigation mechanism within the system's design. Table I summarises relevant threats and mitigation strategies addressed in our proposed architecture. For each category, the corresponding defensive technique (e.g., ECC-based mutual authentication, nonce-driven freshness, role-based access control) and its security outcome are outlined.

VI. Comparison With Related Studies

Table II presents the comparative analysis of prior studies with our work by examining five critical dimensions: primary focus, BC infrastructure, NFT adoption, IoT integration, and industry context. Several earlier efforts concentrate predominantly on counterfeiting [3], [8], [13], while others emphasise traceability [5], [9], [14], and one singular study [10] centres on broader asset security and authentication within smart-city environments. In terms of blockchain platforms, Ethereum dominates the landscape (used by [8], [9], [14]), whereas references [3] and [13] employ more restrictive environments—a private chain in [3] and a consortium/permissioned blockchain in [13]—and [10] leverages the Goerli testnet. Notably, every listed study, including the current one, incorporates NFTs to create unique digital twins, underscoring the consensus that NFTs are indispensable for guaranteeing item uniqueness and thwarting duplication. However, IoT integration varies widely: some works use environmental sensors (e.g., RFID in [3]), a few report no IoT involvement [5], [8], [9], [10], [14], and only [13] utilise hardware-level PUF tags for item authentication rather than conventional sensor data.

The choice of supply chain domain further differentiates these studies: prior work spans general manufacturing [3], [5], healthcare [8], seed distribution [9], smart cities [10], hardware components [13], and unmanned aerial vehicle manufacturing [3]. In contrast, the present study fills an important gap by targeting the luxury goods sector, a market uniquely susceptible to counterfeiting and brand dilution. This comparison reveals four overarching insights: first, NFTs are unanimously adopted as the mechanism of choice for non-fungible digital representation; second, IoT strategies diverge between environmental sensing, hardware PUF authentication, and, in many cases, no IoT involvement; third, BC deployments range from fully public Ethereum networks to private or permissioned architectures; and fourth, no investigations have addressed high-value luxury items, positioning the current work's focus on Ethereum-based NFTs and PUF tags in the luxury domain as both novel and timely.

VII. Conclusion and Future Work

This study presents a novel and secure framework for resilient and traceable supply chains. The framework delivers a comprehensive provenance system that fuses physical security via PUF with BC-backed digital authenticity employing NFT. Our proposed framework uniquely identifies an item by linking the PUF ID to product metadata. The product metadata is recorded in an immutable ledger after on-chain authentication. The framework offers real-time transfer of ownership and location updates related to product journey, while licensed certifiers issue cryptographically verifiable digital certificates on-chain, indicating the proof of authenticity of a product.

The current framework is based on simulated PUF tags and ECC key pairs, which cannot expose physical environmental variations that occur in tags. Further, analysis of gas cost and latency for various smart contract functions was performed on a local Hardhat BC node. These values may vary when observed on testnets and mainnet. To mitigate scalability issues, layer 2 BC or off-chain storage would be viable options to register large-scale batches of PUF-tagged products. Also, the revokeRole() function is not implemented in the current smart contract to handle compromised nodes.

For future work, the framework can be extended for decentralised data analytics (e.g., fake product detection or supply chain demand forecast), using the federated learning paradigm to maintain privacy and security of edge-specific information. Additionally, alternative token standards, such as multi-token (ERC-1155), will be examined for their capabilities in batched or grouped traceability. The proposed architecture can be coupled with other lightweight blockchains to mitigate scalability challenges in large-scale applications. Also, an extension to the smart contract for the implementation of the revokeRole() function to suspend the access rights of a compromised node to sign or validate new transactions.

References

[1] L. Aniello, B. Halak, P. Chai, R. Dhall, M. Mihalea, and A. Wilczynski, "Towards a supply chain management system for counterfeit mitigation using blockchain and PUF," 2019, *arXiv:1908.09585*.

[2] M. M. Queiroz and S. F. Wamba, "Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA," *Int. J. Inf. Manage.*, vol. 46, pp. 70–82, Jun. 2019.

[3] G. Narayanan, I. Cvitić, D. Peraković, and S. Raja, "Role of blockchain technology in supplychain management," *IEEE Access*, vol. 12, pp. 19021–19034, Jun. 2024.

[4] J. Davies, H. Sharifi, A. Lyons, R. Forster, and O. K. S. M. Elsayed, "Non-fungible tokens: The missing ingredient for sustainable supply chains in the metaverse age?" *Transp. Res. Part E: Logistics Transp. Rev.*, vol. 182, 2024, Art. no. 103412.

[5] N. Habtemichael, H. Wicaksono, and O. F. Valilai, "NFT-based digital twins for tracing value-added creation in manufacturing supply chains," *Procedia Comput. Sci.*, vol. 232, pp. 2841–2846, 2024.

[6] A. Falcone, C. Felicetti, A. Garro, and D. Saccà, "PUF-based smart tags for supply chain management," in *Proc. ACM Int. Conf. Comput. Front.*, pp. 261–264. 2021.

[7] M. N. Alatawi, "EdgeGuard-IoT: 6G-enabled edge intelligence for secure federated learning and adaptive anomaly detection in industry 5.0," *Comput., Mater. Continua*, vol. 85, no. 1, pp. 695–727, 2025.

[8] S. S. Kumar, K. Singh, and A. Bubber, "Manufacture and registration of products in healthcare supply chain using NFTS," in *Proc. 4th Int. Conf. Technol. Adv. Comput. Sci. (ICTACS)*, Piscataway, NJ, USA: IEEE Press, 2024, pp. 1136–1141.

[9] R. Ahuja, S. Chugh, and R. Singh, "SeedChain: A secure and transparent blockchain-driven framework to revolutionize the seed supply chain," *Future Internet*, vol. 16, no. 4, p. 132, 2024.

[10] U. Khalil, M. Uddin, O. A. Malik, and O. W. Hong, "A novel NFT solution for assets digitization and authentication in cyber-physical systems: Blueprint and evaluation," *IEEE Open J. Comput. Soc.*, vol. 5, pp. 131–143, 2024.

[11] L. Wang, W. Sun, J. Zhao, X. Zhang, C. Lu, and H. Luo, "A non-fungible token and blockchain-based cotton lint traceability solution," *Appl. Sci.*, vol. 14, no. 4, 2024, Art. no. 1610.

[12] P. Helo, Y. Hao, and A. Gunasekaran, "Use of non-fungible tokens in operations and supply chain management," *Int. J. Prod. Res.*, vol. 63, no. 14, pp. 5099–5121, 2025.

[13] S. Balla, Y. Zhao, and F. Koushanfar, "ICtoken: An NFT for hardware IP protection," 2024, *arXiv:2412.06726*.

[14] D. Hawashin, M. Nemer, K. Salah, R. Jayaraman, D. Svetinovic, and E. Damiani, "Blockchain and NFT-based traceability and certification for UAV parts in manufacturing," *J. Ind. Inf. Integration*, vol. 39, 2024, Art. no. 100597.

Biographies

Antonella Guzzo (Senior Member, IEEE) is an Associate Professor of computer engineering with DIMES Department, University of Calabria, Italy. Since 2018, she has the Italian national scientific qualification to Full Professor, SSD ING-INF/05, sector 09/H1. Previously, she was a Research Fellow with the High Performance Computing and Networks Institute (ICAR-CNR), National Research Council, Italy. She is member of the Ph.D. Board in ICT with the University of Calabria. Her research interests include process mining, data mining, artificial intelligence and deep learning. She authored more than 70 papers in top international journals and conferences. She serves as reviewer for over 20 international journals and as a Program Committee (PC) Member in many international conferences and workshops, including IJCAI (2020–2021) and AAAI (2020–2021) and BPM, ICPM. Since 2005, she has been involved in national and international research projects as member and/or responsible of unit and/or responsible of project. She is also an Active Member in the process mining community, since was member of the IEEE task force in process mining and she was member of the IEEE Working Group for the definition of the Standard XES - eXtensible Event Stream.

Domenico Sacca (Senior Member, IEEE) is an Emeritus Professor of computer engineering with the University of Calabria, where he served as a Full Professor from 1987 to 2021. He has held major leadership roles, including Director of ICAR-CNR, the Institute for High Performance Computing and Networking of the Italian National Research Council, and the President of ICT-SUD, a competence center in computing and telecommunications in Southern Italy. He was a Visiting Scientist with IBM Almaden, UCLA, and ICSI Berkeley, and a Scientific Consultant for MCC, United States. He is a Senior Member of ACM. He is the Founder of SEBD in 1993, he coordinated its Steering Committee until 2021 and is currently a Emeritus Member.

Giancarlo Fortino received the Ph.D. degree in systems and computer engineering from Unical, in 2000. He is a Professor of computer engineering with DIMES Department of University of Calabria, Italy. His research interests include wearable computing, IoT and applied artificial intelligence. He is a Highly Cited Researcher 2020–2025 by Clarivate in Computer Science. He is an author of 750+ papers in top-level journals, conferences & book series. He is the Founding Series Editor of the IEEE Press Book Series on Human-Machine Systems and AE of many premier IEEE Transactions/Journals. He is a Co-Founder-CEO of SenSysCal Srl, Unical spinoff on IoT systems. He is the Vice President of cybernetics of the IEEE SMC society.

Fahed Alkhabbas received the bachelor's degree in computer information technology from Arab American University, Palestine, the master's degree in computer science from Trento University, Italy, and the Ph.D. degree in computer science from Malmö University. He is currently a Senior Lecturer and a Researcher with the Department of Computer Science and Media Technology, Malmö University, Sweden. He is also affiliated with the Sustainable Digitalisation Research Centre, Malmö University, Sweden. He has more than seven years of industrial experience in software development, during which he led several teams in international organizations and companies, such as the United Nations, Tetra Tech DPK, GVC-Italia, and FreightOS. His research interests include software architecture, multiagent systems, federated learning, and Internet of Things.

Fiza Siyal received the B.E. degree in software engineering and the M.E. degree in information technology from Mehran University of Engineering & Technology (MUET), Jamshoro, Pakistan. She is currently working toward the Ph.D. degree with the University of Calabria, Italy. She is an Assistant Professor with the Department of Software Engineering, Quaid-e-Awam University of Engineering, Science and Technology (QUEST), Nawabshah, Pakistan. Her research focuses on distributed ledger technologies, PUFs, and AI solutions to provide provenance assurance and to identify counterfeits within the supply chains. Additionally, she is involved in blockchain security research with a focus on applying AI to detect vulnerabilities in smart contracts.

Open Access funding provided by 'Universitã della Calabria 2025-2027 Deposit Account' within the CRUI CARE Agreement