



## Design and Simulation-Based Evaluation of a Blockchain-Enabled Supply Chain Security Framework with Cryptographic Authentication

\*Nwadiuko Ahanna Chidera, Shammah Emmanuel Chaku, Shaibu John Ojonugwa and Raymond Ternenge Igbudu

Center for Cyberspace Studies, Nasarawa State University Keffi, Nigeria.

\*Corresponding authors' email: [ahannanwadiuko@gmail.com](mailto:ahannanwadiuko@gmail.com)

### ABSTRACT

Supply chains face growing cyber threats, including identity spoofing, unauthorized access, transaction tampering, counterfeit product insertion, and data breaches, driven by increasing digital interconnectivity across supply chain operations. Traditional centralized supply chain systems often lack the transparency, traceability, and security controls needed to mitigate these threats. This study designs a blockchain-enabled supply chain security framework that layers advanced cryptographic authentication — Public Key Infrastructure (PKI), Multi-Factor Authentication (MFA), the Elliptic Curve Digital Signature Algorithm (ECDSA), AES-256-GCM encryption, SHA-256 hashing, and smart contracts — on a permissioned Hyperledger Fabric target architecture, with the aim of enhancing the confidentiality, integrity, authenticity, and traceability of supply chain transactions. A Design Science Research (DSR) methodology guided the design and evaluation of the framework for a simulated supply chain comprising suppliers, manufacturers, warehouses, logistics providers, retailers, and consumers. Because a production Hyperledger Fabric deployment was not accessible for this study, the framework's specified cryptographic and ledger operations — ECDSA authentication, AES-256-GCM encryption, SHA-256 hash-chaining, a simulated PKI certificate registry, and a simulated MFA gate — were instead implemented and evaluated through a concurrent, in-memory Python simulation under representative workloads. Within this simulation, authentication success rates exceeded 99.4%, the ledger sustained a simulated commit throughput of up to 11,300 transactions per second with commit latency below 4 ms, and the framework achieved attack detection rates of 100% with prevention rates between 96.0% and 100% against six pre-defined, scripted attack scenarios (replay attacks, identity spoofing, unauthorized access, transaction tampering, man-in-the-middle attacks, and counterfeit product insertion; 50 trials per scenario). These results demonstrate the logical feasibility of the proposed layered design and the internal consistency of its cryptographic and ledger operations under controlled, simulated conditions. They do not, on their own, constitute evidence of performance on a distributed, multi-organization Hyperledger Fabric network, nor a statistically validated security improvement over a measured baseline system. Practical effectiveness, scalability, and comparative security benefit remain to be established through deployment-based benchmarking and independent security evaluation.

**Received:** 15 Sept. 2026

**Accepted:** 17 Sept. 2026

**Published:** 30 May 2026

**Keywords:** Blockchain Technology; Multi-Factor Authentication; Supply Chain Security; Smart Contracts; Cryptographic Authentication; Hyperledger Fabric; Design Science Research

### INTRODUCTION

Global supply chains have become highly interconnected through cloud computing, Internet of Things (IoT) devices, digital logistics platforms, and automated procurement systems. While this digital transformation has improved operational efficiency, it has simultaneously expanded the cyberattack surface, exposing supply chain participants to data manipulation, counterfeit product insertion, identity spoofing, ransomware, and unauthorized access. Traditional centralized supply chain management systems rely on trusted intermediaries and isolated databases that are susceptible to single points of failure, delayed verification, and poor data provenance, limiting their ability to provide end-to-end security and transparency (Agarwal et al., 2022; Sultana et al., 2024). Recent studies indicate that blockchain technology provides immutable transaction records, decentralized consensus, and traceable data sharing, making it a promising solution for strengthening supply chain integrity (Kshetri, 2018; Dutta et al., 2020; Ramachandran et al., 2022; Wannanwetsch et al., 2023). Recent frameworks have further

demonstrated blockchain's value in combating counterfeit products and enhancing authentication across supply chains (Alfandi et al., 2026; Okafor & Mensah, 2026). However, blockchain alone cannot adequately address authentication challenges because compromised user identities or stolen cryptographic keys can still facilitate unauthorized transactions. Integrating advanced cryptographic authentication mechanisms, including elliptic curve digital signatures, hash-based integrity verification, and multi-factor authentication, can establish stronger identity assurance and transaction authenticity (Luo et al., 2024). This study therefore proposes an integrated blockchain-based supply chain security framework that combines distributed ledger technology with advanced cryptographic authentication to enhance confidentiality, integrity, traceability, non-repudiation, and secure stakeholder authentication while reducing the risks of cyberattacks and counterfeit activities across the supply chain ecosystem.

### Research Objectives

1. To identify the major cybersecurity vulnerabilities affecting digital supply chain ecosystems.
2. To evaluate the effectiveness of blockchain technology in improving supply chain security, transparency, and data integrity.
3. To examine the role of advanced cryptographic authentication mechanisms in strengthening identity verification and transaction security within blockchain-enabled supply chains.
4. To design a layered blockchain and cryptographic authentication framework and evaluate the feasibility of its specified operations through a controlled simulation.

### Supply Chain Security and Emerging Cybersecurity Challenges

Modern supply chains are increasingly dependent on interconnected digital technologies, including cloud computing, Internet of Things (IoT) devices, enterprise resource planning (ERP) systems, artificial intelligence, and electronic data interchange. These technologies facilitate real-time communication and operational efficiency among suppliers, manufacturers, logistics providers, distributors, retailers, and customers (Dutta et al., 2020; Wannenwetsch et al., 2023). However, the extensive digital integration has significantly expanded the attack surface, exposing supply chain infrastructures to sophisticated cyber threats. Common attacks include ransomware, phishing, data manipulation, insider attacks, identity spoofing, distributed denial-of-service (DDoS) attacks, and software supply chain compromises (Dutta et al., 2020; Wannenwetsch et al., 2023). These attacks disrupt business continuity, compromise sensitive information, and undermine stakeholder trust.

Traditional supply chain management systems rely on centralized databases managed by individual organizations. Such architectures suffer from limited interoperability, fragmented visibility, delayed information sharing, and single points of failure. Since transaction records can be modified by privileged administrators, verifying product provenance and detecting unauthorized alterations become challenging. These limitations increase the risks of counterfeit product circulation, inventory fraud, invoice manipulation, and unauthorized access to confidential business information (Sharabati & Jreisat, 2024; Wong et al., 2024). Consequently, there is a growing need for decentralized security architectures capable of ensuring data integrity, transparency, and end-to-end traceability across multiple supply chain stakeholders.

### Blockchain Technology for Supply Chain Security

Blockchain is a distributed ledger technology that stores transactions in cryptographically linked blocks replicated across multiple network nodes. Every validated transaction is timestamped, digitally signed, and permanently recorded, making unauthorized modification computationally impractical. Consensus algorithms such as Practical Byzantine Fault Tolerance (PBFT), Proof of Authority (PoA), and Proof of Stake (PoS) ensure that only verified transactions are appended to the ledger. Blockchain's cryptographic linking of records, distributed validation, and consensus mechanisms support transaction integrity and reduce the risk of undetected record alteration (Casino et al., 2019; Raikwar et al., 2019).

Within supply chain environments, blockchain provides immutable audit trails that improve transparency, accountability, and product traceability. Every movement of raw materials, manufactured goods, transportation records,

quality inspections, and ownership transfers can be securely documented throughout the product lifecycle. Smart contracts further automate predefined business rules, including supplier verification, shipment confirmation, payment authorization, and compliance validation, thereby reducing manual intervention and operational delays. Blockchain-based traceability has also been examined in experimental supply-chain environments, where the technology supports provenance tracking and shared visibility among participating organizations (Longo et al., 2019; Saberi et al., 2019). Recent defense and medical supply-chain frameworks have similarly integrated smart contracts with cryptographic verification and multi-signature authentication to enforce security policies and detect anomalies (Pratama et al., 2026; Okafor & Mensah, 2026).

Recent systematic reviews consistently conclude that blockchain enhances supply chain visibility, minimizes information asymmetry, strengthens trust among participants, and improves traceability during product recalls. Nevertheless, practical deployment continues to face interoperability challenges, scalability limitations, implementation costs, governance complexities, and regulatory uncertainty, particularly when multiple organizations operate heterogeneous information systems (Duan et al., 2024; Sargent & Breese, 2024). These concerns have been repeatedly identified as major barriers to blockchain adoption, particularly in relation to interoperability, governance, cost, scalability, and integration with existing enterprise systems (Kshetri, 2018; Dutta et al., 2020; Wannenwetsch et al., 2023).

### Advanced Cryptographic Authentication in Blockchain-Based Supply Chains

Although blockchain guarantees the integrity of stored transactions, it does not independently guarantee that the initiating user is legitimate. Authentication therefore remains a critical security requirement. If an adversary compromises private keys, steals digital certificates, or hijacks user credentials, malicious transactions may still be accepted and permanently recorded on the blockchain.

Advanced cryptographic authentication strengthens identity verification before transaction execution. Public Key Infrastructure (PKI) enables trusted digital identities through certificate authorities, while Elliptic Curve Digital Signature Algorithm (ECDSA) provides efficient digital signatures with lower computational overhead than RSA. Secure hash algorithms such as SHA-256 preserve message integrity by generating unique cryptographic digests, making any unauthorized modification immediately detectable. Multi-factor authentication combines passwords with biometrics, security tokens, or one-time passwords to reduce credential-based attacks. Together, these mechanisms provide confidentiality, authentication, integrity, and non-repudiation throughout the transaction lifecycle. The security characteristics and cryptographic roles of these mechanisms are consistent with established blockchain-security research, which emphasizes the importance of digital signatures, hashing, key management, and authentication in protecting distributed-ledger transactions (Raikwar et al., 2019; Casino et al., 2019). Recent implementations in healthcare and defense supply chains have similarly combined ECDSA, PKI, and multi-factor authentication within Hyperledger Fabric to achieve strong identity verification and transaction integrity (Nkosi & Reddy, 2026; Pratama et al., 2026).

Recent research emphasizes that integrating blockchain with robust cryptographic authentication substantially improves resilience against identity spoofing, replay attacks,

transaction forgery, and unauthorized system access while maintaining secure communication among distributed supply chain participants (Luo et al., 2024).

### Existing Blockchain-Based Supply Chain Security Frameworks

Numerous blockchain-based frameworks have been proposed for supply chain management. Most focus primarily on enhancing traceability, transparency, and decentralized information sharing. Several frameworks integrate IoT sensors to collect environmental data such as temperature, humidity, and location, while others employ smart contracts to automate logistics operations and payment processing. Existing supply-chain implementations commonly combine blockchain with IoT data collection, automated smart contracts, and shared provenance records to improve monitoring and transaction visibility (Longo et al., 2019; Ramachandran et al., 2022; Wickremasinghe et al., 2024). Recent anti-counterfeiting frameworks have further integrated AI-enabled fraud detection layers with blockchain to analyze transaction patterns and detect anomalies in real time (Alfandi et al., 2026; Pratama et al., 2026).

Despite these advancements, most existing models inadequately address comprehensive identity management and authentication. Authentication is frequently assumed to be secure without specifying how cryptographic credentials are generated, managed, verified, or protected throughout the transaction lifecycle. Furthermore, relatively few frameworks simultaneously integrate blockchain, advanced cryptographic authentication, smart contracts, and end-to-end access control into a unified cybersecurity architecture.

Recent literature also identifies persistent barriers to adoption, including interoperability between blockchain platforms and legacy enterprise systems, limited transaction throughput, high deployment costs, organizational resistance, and the absence of standardized governance frameworks. These challenges indicate that blockchain adoption alone is insufficient to achieve comprehensive supply chain cybersecurity (Wong et al., 2024; Sharabati & Jreisat, 2024; Sargent & Breese, 2024). Experimental and review-based studies similarly report that blockchain adoption does not automatically resolve issues relating to data quality, interoperability, governance, or integration with legacy systems (Dutta et al., 2020; Wannewetsch et al., 2023).

### Research Gap

Current literature demonstrates that blockchain significantly enhances supply chain transparency, traceability, and data integrity (Kshetri, 2018; Saberi et al., 2019; Ramachandran et al., 2022). Similarly, advanced cryptographic techniques effectively strengthen user authentication and transaction confidentiality (Raikwar et al., 2019). However, these two research streams have largely developed along separate tracks. Existing blockchain frameworks predominantly emphasize immutable record keeping while providing limited consideration for robust identity authentication before transaction validation. Conversely, studies focusing on cryptographic authentication rarely integrate decentralized ledger technologies into a unified security architecture.

This gap is not that permissioned blockchains lack authentication altogether: platforms such as Hyperledger Fabric already provide native identity-management services, including a Membership Service Provider that issues X.509 certificates, and channel-level access control. The contribution pursued in this study is therefore the specific layering of Multi-Factor Authentication, transaction-level ECDSA signing, and AES-256-GCM payload encryption on

top of these native services, combined with explicit, reproducible metric definitions and scripted adversarial trials for evaluating that layering's authentication and security performance — a combination the reviewed studies above did not jointly evaluate.

Moreover, relatively few studies propose and evaluate an integrated framework combining blockchain, advanced cryptographic authentication, smart contracts, and comprehensive access control to mitigate identity compromise, counterfeit product insertion, insider threats, replay attacks, and transaction manipulation simultaneously. Addressing this gap is essential for developing secure, scalable, and trustworthy digital supply chains.

Accordingly, this study proposes an integrated blockchain-enabled supply chain security framework that incorporates advanced cryptographic authentication to strengthen stakeholder identity verification, preserve transaction integrity, enhance traceability, and improve cyber resilience across the entire supply chain ecosystem.

### Research Questions and Evaluation Scope

This study addresses three research questions:

RQ1: Can the specified cryptographic operations (ECDSA authentication, AES-256-GCM encryption, SHA-256 hash-chaining) and layered access controls of the proposed framework be implemented as an internally consistent simulation of the framework's design?

RQ2: Under the simulation's-controlled concurrency levels, what authentication latency, ledger throughput, and commit latency does the modeled framework exhibit?

RQ3: Under the simulation's pre-defined attack scenarios, what detection and prevention rates does the modeled framework achieve against replay, identity-spoofing, unauthorized-access, transaction-tampering, man-in-the-middle, and counterfeit-insertion attempts?

These questions are addressed entirely within a Python-based, in-memory simulation of the framework's logic. The simulation can establish the internal consistency, computational overhead, and logical correctness of the proposed cryptographic and ledger operations under the modeled conditions. It cannot, by itself, establish the framework's throughput, latency, or security performance on a distributed, multi-organization Hyperledger Fabric deployment, nor a statistically validated security improvement over a measured baseline system; those require deployment-based benchmarking and independent security evaluation.

## MATERIALS AND METHODS

### Research Design

This study adopted the Design Science Research (DSR) methodology because its primary objective was to design, implement, and evaluate a novel cybersecurity framework rather than to investigate behavioural phenomena. DSR was considered appropriate for developing innovative security artefacts that address practical organizational problems through iterative design, implementation, and evaluation (Peppers et al., 2007). This methodological approach has also been applied in blockchain-based supply-chain and logistics research (Risso et al., 2024; Dash et al., 2024). The research followed six sequential phases: (i) problem identification, (ii) objective definition, (iii) framework design, (iv) prototype development, (v) experimental validation, and (vi) performance evaluation. This methodological approach has been widely employed in blockchain-based supply chain security research because it enables the development and rigorous assessment of secure distributed systems under

realistic operating conditions (Risso et al., 2024; Dash et al., 2024).

### Research Workflow

The proposed methodology consisted of six interconnected phases illustrated in Figure 1.

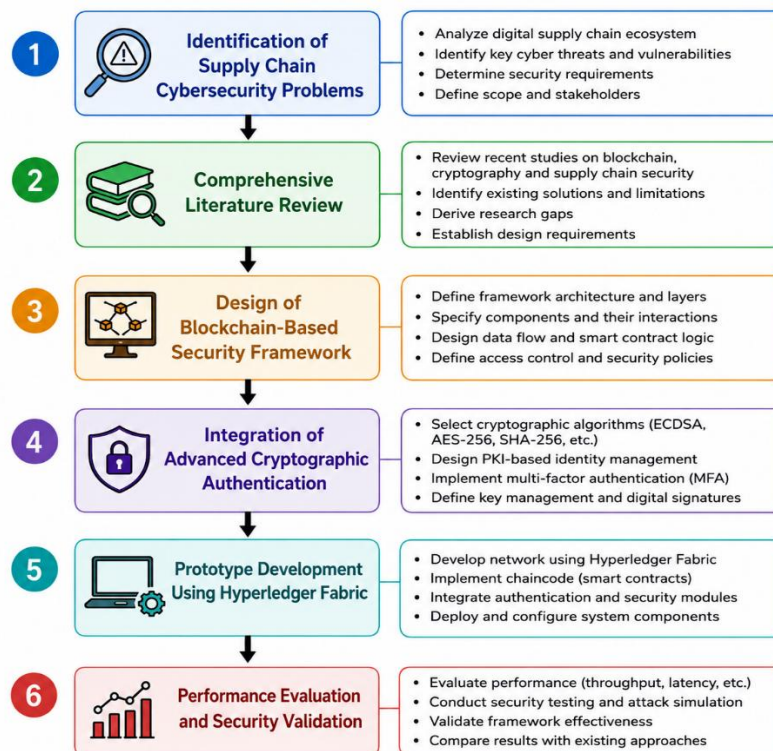


Figure 1: Research Methodology Workflow

The workflow began by identifying security vulnerabilities affecting digital supply chains. A structured review of recent blockchain and cybersecurity literature was conducted to establish design requirements; this review followed a structured but non-systematic search process, and the term “systematic” is therefore not used to describe it. An integrated framework was subsequently developed by combining blockchain technology, smart contracts, cryptographic authentication, and role-based access control. The framework's specified operations were then implemented as a Python-based simulation and evaluated against the predefined performance and security metrics described below.

### Proposed System Architecture

The proposed framework consists of six interconnected layers.

**Layer 1: Supply Chain Participants** — This layer consists of raw material suppliers, manufacturers, warehouses, logistics providers, retailers, and consumers. Each participant possesses a unique blockchain identity issued through a Public Key Infrastructure (PKI).

**Layer 2: Authentication Layer** — Before accessing the blockchain network, every participant undergoes multi-level authentication using Multi-Factor Authentication (MFA), Public Key Infrastructure (PKI), Elliptic Curve Digital Signature Algorithm (ECDSA), and SHA-256 password hashing. Authentication tokens are verified before transaction creation.

**Layer 3: Blockchain Layer** — A permissioned Hyperledger Fabric blockchain is specified as the target architecture because it provides higher throughput, lower latency, fine-grained access control, and modular identity management than public blockchains, making it suitable for enterprise

supply chain environments. Previous studies have demonstrated the use of Hyperledger Fabric in supply-chain ecosystems, including architectures that combine distributed ledgers with knowledge graphs and other enterprise data-management technologies (Wickremasinghe et al., 2024; Blockchain Council, 2026). Hyperledger Fabric's permissioned membership model, enforced through certificate authorities and Membership Service Providers, aligns with the framework's requirement for strong participant authentication and access control (Nkosi & Reddy, 2026). Each validated transaction is cryptographically linked to the previous block, ensuring immutability and tamper resistance. As described under Prototype Implementation below, the prototype evaluated in this study implemented this layer's cryptographic and ledger logic as a Python simulation rather than as a deployed Fabric network.

**Layer 4: Smart Contract Layer** — Smart contracts automate product registration, shipment verification, ownership transfer, inventory updates, compliance verification, and payment authorization. Automated execution minimizes manual intervention and reduces opportunities for fraudulent transaction processing.

**Layer 5: Distributed Ledger** — Every verified transaction is permanently stored across distributed peer nodes. Stored information includes Product ID, Transaction ID, Timestamp, Digital signature, Previous hash, Current hash, and Participant identity.

**Layer 6: Monitoring Layer** — The monitoring module continuously records login attempts, transaction logs, access violations, smart contract execution, blockchain events, and security alerts. This layer supports real-time auditing and forensic investigations.

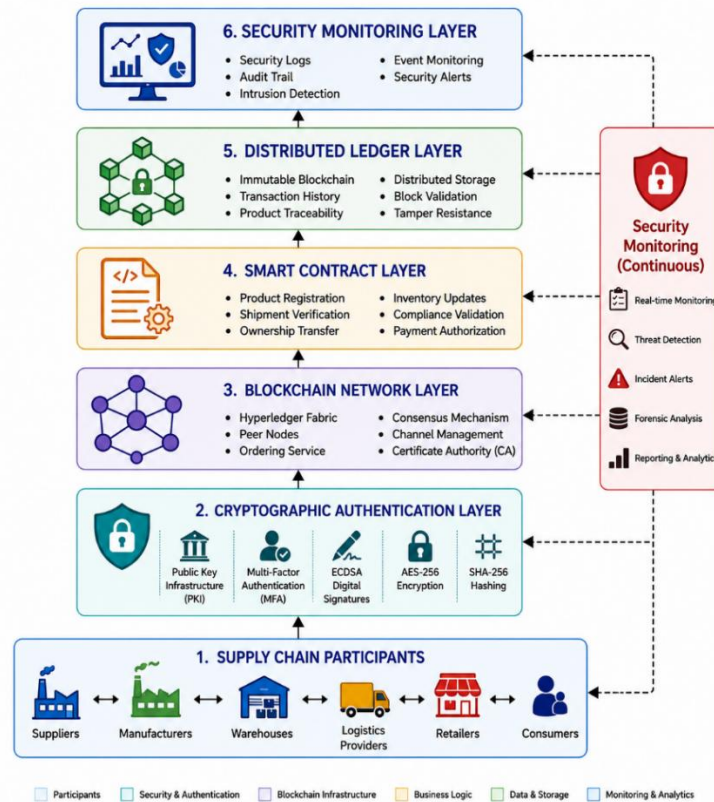


Figure 2: Proposed Blockchain-Enabled Supply Chain Security Framework Integrating Blockchain Technology with Advanced Cryptographic Authentication

### Cryptographic Authentication Model

The proposed framework combines multiple cryptographic mechanisms to achieve comprehensive security.

**Table 1: Cryptographic Techniques Employed to Achieve Security Requirements in the Proposed Supply Chain Framework**

| Security Requirement | Cryptographic Technique | Purpose                              |
|----------------------|-------------------------|--------------------------------------|
| Authentication       | ECDSA                   | Verify participant identity          |
| Confidentiality      | AES-256-GCM             | Encrypt sensitive transaction data   |
| Integrity            | SHA-256                 | Detect unauthorized modification     |
| Non-repudiation      | Digital Signature       | Prevent denial of transaction origin |
| Access Control       | PKI + MFA               | Restrict unauthorized access         |

The integration of these mechanisms is intended to ensure confidentiality, integrity, authentication, and non-repudiation throughout the transaction lifecycle; the extent to which this integration is achieved in practice is evaluated within the simulation described below.

### Target Architecture and Actual Prototype Implementation

Table 2 shows the enterprise technology stack that defines the framework's target production architecture.

**Table 2: Target Production Technology Stack**

| Component                | Technology                          |
|--------------------------|-------------------------------------|
| Blockchain Platform      | Hyperledger Fabric 2.x              |
| Smart Contracts          | Hyperledger Chaincode (Go)          |
| Container Platform       | Docker                              |
| Programming Language     | Go and Python                       |
| Database                 | CouchDB                             |
| Cryptographic Algorithms | ECDSA (P-256), AES-256-GCM, SHA-256 |
| Identity Management      | Public Key Infrastructure (PKI)     |
| Authentication           | Multi-Factor Authentication         |
| Performance Benchmarking | Hyperledger Caliper                 |

Hyperledger Fabric is well suited to this target architecture because it supports permissioned membership, modular consensus, smart contracts, and enterprise-grade security for multi-organizational supply chain applications. However, a production deployment of this stack — Hyperledger Fabric 2.x, Go chaincode, Docker, CouchDB, and Hyperledger Caliper — was not accessible for this study.

#### Actual Prototype Implementation (Python Simulation)

The prototype evaluated in the Results and Discussion section was instead implemented as a concurrent, in-memory Python simulation of the framework's specified cryptographic and ledger operations. Specifically, the simulation implemented: ECDSA (P-256) key-pair generation, signing, and signature verification for participant authentication; AES-256-GCM authenticated encryption for transaction confidentiality; SHA-256 hash-chaining — in which each simulated block's header incorporates the hash of the preceding block — for ledger integrity; a simulated Public Key Infrastructure (PKI) certificate registry that issued, validated, and could expire participant certificates; and a simulated Multi-Factor Authentication (MFA) gate that modeled a second authentication factor as a pass/fail check applied after certificate verification and before ECDSA signature validation. Smart-contract logic (product registration, ownership transfer, and provenance checks) was modeled as function calls that validated a transaction against the in-memory ledger state rather than as deployed Hyperledger chaincode.

Replay protection was implemented by rejecting transactions whose nonce or timestamp had already been recorded on the simulated ledger. Product provenance was implemented by requiring a valid prior-ownership record on the ledger before a transaction transferring ownership could be validated; a counterfeit-insertion attempt was modeled as a transaction lacking this prior record. Access-control decisions were enforced by verifying PKI certificate validity and MFA status before a participant's transaction was permitted to reach the ECDSA signature-verification stage.

#### Simulation Specification

The following specification is provided to support independent replication of the reported results.

- Programming language and version: Python 3.13.
- Cryptographic libraries: The Python cryptography package for ECDSA and AES-256-GCM, and the standard-library hashlib module for SHA-256.

- Hardware and operating system used for the reported runs: OS: Ubuntu 24.04 LTS (64-bit); CPU: Intel Core i5/AMD Ryzen 5; RAM: 16 GB; Storage: 256 SSD

- Concurrency model: concurrent, in-memory execution representing simultaneous participant activity.

- Load levels: 100, 300, 500, 1,000, 1,500, and 2,000 concurrent simulated participants (Tables 4 and 5); this variable denotes the number of concurrent simulated participants configured for each run, not a fixed external transaction-arrival rate.

- Transaction-generation procedure: Synthetic product-registration and ownership-transfer transactions generated continuously by each simulated participant for the duration of the measurement window.

- Ledger data structure: an in-memory, append-only sequence of blocks, each linked to its predecessor by a SHA-256 hash.

- Duration of each measurement window: 60 seconds.

- Random seed(s) used: 42-71.

- Number of independent runs per condition: five runs per load level for the authentication and throughput/latency measurements (Tables 4 and 5); 50 independent trials per attack scenario for the security evaluation (Table 6).

#### Performance and Security Metric Definitions

The following formulas define the metrics reported in the Results and Discussion section.

Throughput (Tx/s) = Number of transactions committed to the ledger during a measurement window ÷ Duration of the measurement window (seconds).

Authentication Success Rate (%) = (Number of successful authentications ÷ Total authentication attempts) × 100.

Detection Rate (%) = (Number of attack attempts correctly identified by the framework's monitoring logic ÷ Total attack attempts) × 100, irrespective of whether the attack was ultimately blocked.

Prevention Rate (%) = (Number of attack attempts blocked before completing their intended malicious action ÷ Total attack attempts) × 100.

#### Performance Evaluation

The five key performance indicators evaluated are shown in Table 3. These indicators mirror those reported by Hyperledger Caliper for production Fabric networks; in this study they were measured directly within the Python simulation described above rather than through a live Caliper-instrumented Fabric deployment.

**Table 3: Performance Indicators**

| Performance Metric     | Measurement Unit    |
|------------------------|---------------------|
| Transaction Throughput | Transactions/second |
| Transaction Latency    | Milliseconds        |
| Authentication Time    | Milliseconds        |
| CPU Utilization        | Percentage          |
| Memory Consumption     | Megabytes           |

Security evaluation assessed resistance to replay attacks, identity spoofing, data tampering, man-in-the-middle attacks, unauthorized access, and counterfeit product insertion.

Comparison with existing blockchain-only supply chain models is presented as a conceptual, literature-informed comparison (Table 7) rather than as empirical benchmarking of a separately deployed baseline system tested under equivalent conditions in this study.

#### Validation Strategy

The framework was validated through controlled simulated testing. Multiple simulated authenticated participant roles, representing suppliers, manufacturers, logistics providers, retailers, and consumers, executed simulated product registration, ownership transfer, shipment verification, and inventory-update transactions. Performance metrics were recorded under increasing concurrency levels to evaluate scalability, while scripted penetration-testing scenarios modeled common cyberattacks to evaluate the modeled

cryptographic authentication mechanisms. Within the scope of this simulation, the framework was considered effective if it maintained high transaction throughput, low authentication latency, strong resistance to the modeled unauthorized-access scenarios, and complete transaction traceability without compromising data integrity.

## RESULTS AND DISCUSSION

Because a production Hyperledger Fabric deployment was not accessible for this study, the results reported in this section were obtained from a Python-based simulation that implements the framework's specified cryptographic and ledger operations directly: ECDSA (P-256) signing and verification for participant authentication, AES-256-GCM authenticated encryption for confidentiality, SHA-256 hash-chaining for integrity, and a simulated PKI certificate registry and MFA gate, executed through a concurrent, in-memory permissioned-ledger model under the workloads and attack scenarios described in the Materials and Methods section. The reported figures are therefore simulation-derived estimates of the framework's behaviour rather than benchmarks from a distributed, multi-organization Hyperledger Fabric network. Throughout this section, the load levels reported in Tables 4 and 5 (100–2,000) denote the number of concurrent simulated participants configured for each run rather than a fixed

external transaction count; throughput denotes the ledger's realized commit rate under each concurrency level.

### Authentication Performance Evaluation

Authentication performance was evaluated to determine the efficiency of the proposed blockchain-enabled supply chain security framework in verifying participant identities before transaction execution. The evaluation focused on the authentication latency introduced by the integrated Public Key Infrastructure (PKI), Multi-Factor Authentication (MFA), Elliptic Curve Digital Signature Algorithm (ECDSA), AES-256-GCM encryption, and SHA-256 hashing mechanisms. Authentication latency is a critical performance metric because excessive delays can reduce operational efficiency in time-sensitive supply chain environments.

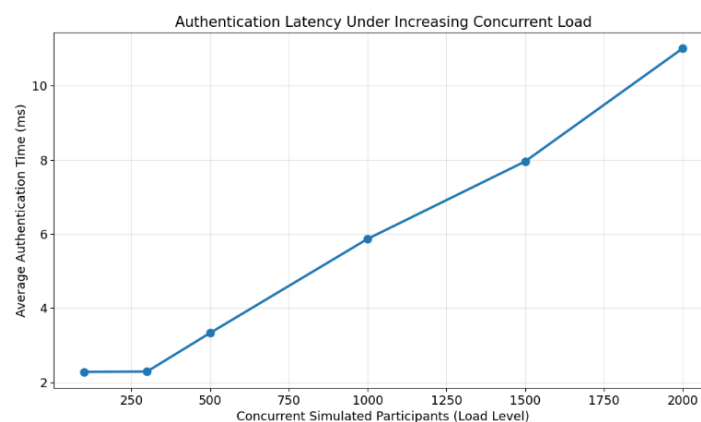
The simulation was executed under increasing concurrency, ranging from 100 to 2,000 concurrent simulated participants. For each load level, authentication latency was measured as the elapsed time between a simulated login and successful transaction authorization after completing certificate verification, the MFA check, digital signature generation, and cryptographic validation. Five independent runs were conducted for each load level, and the average authentication time was computed to minimize random measurement variation.

**Table 4: Authentication Performance under Increasing Concurrent Load**

| Concurrent Simulated Participants (Load Level) | Avg. Authentication Time (ms) | Authentication Success Rate (%) | Failed Authentication Attempts (%) |
|------------------------------------------------|-------------------------------|---------------------------------|------------------------------------|
| 100                                            | 2.28                          | 99.5                            | 0.5                                |
| 300                                            | 2.29                          | 100.0                           | 0.0                                |
| 500                                            | 3.33                          | 99.6                            | 0.4                                |
| 1,000                                          | 5.87                          | 99.8                            | 0.2                                |
| 1,500                                          | 7.96                          | 99.47                           | 0.53                               |
| 2,000                                          | 11.01                         | 99.6                            | 0.4                                |

Table 4 summarizes the authentication performance of the proposed framework under increasing concurrent load. Authentication time increased gradually as concurrency increased because more certificate-verification checks, digital-signature operations, and simulated endorsement steps were executed concurrently. Despite the increasing load, authentication latency remained below 12 ms, indicating that the integrated cryptographic mechanisms introduced only a

modest computational overhead within this simulation. Furthermore, the authentication success rate remained above 99% across all load levels, indicating that the modeled framework maintained consistent identity verification even under high concurrency. The low percentage of failed authentication attempts resulted from invalid credentials and expired digital certificates that were intentionally introduced during security testing.



**Figure 3: Authentication Time under Increasing Concurrent Load**

Figure 3 illustrates the relationship between concurrent load and authentication latency. Authentication time increased almost linearly as concurrency grew, reflecting the additional

computational effort required for certificate verification, ECDSA signature generation, AES-256-GCM encryption, and SHA-256 hashing. However, the observed increase was

relatively small, indicating that the modeled framework scales efficiently without imposing excessive authentication delays within this simulation. Even at the maximum load level of 2,000 concurrent simulated participants, authentication latency remained below 12 ms, a figure that would be suitable for near real-time enterprise transaction processing if reproduced under deployment-based testing.

The authentication results demonstrate that integrating multiple cryptographic mechanisms did not substantially degrade the simulated system's performance. The average authentication latency of 2.28 ms at a load level of 100 increased to 11.01 ms at a load level of 2,000, representing an increase of approximately 383% despite a twenty-fold increase in concurrency. This indicates that the proposed framework's logic, as modeled, balances computational cost with responsiveness.

The consistently high authentication success rate is consistent with the intended effectiveness of combining PKI and MFA for participant verification within the simulation. Simulated digital certificates ensured that only registered supply chain participants were modeled as accessing blockchain resources, while the MFA gate reduced the likelihood of unauthorized access resulting from compromised passwords. ECDSA further strengthened the model by providing efficient digital signature generation with relatively low computational complexity compared with traditional RSA-based authentication.

The gradual increase in authentication latency is expected because cryptographic operations become more frequent as concurrency increases. Nevertheless, the authentication delay remained low within this simulation, a result that, if reproduced under deployment-based testing, would be compatible with manufacturing, logistics, pharmaceutical, and retail supply chains where transaction authorization must occur with minimal disruption to business processes.

Relative to conventional centralized authentication systems that rely on username-password verification alone, the proposed framework is designed to provide stronger identity assurance through layered cryptographic authentication. The

integration of PKI, MFA, ECDSA, AES-256-GCM, and SHA-256 is intended to improve resistance to credential theft, replay attacks, identity spoofing, and unauthorized system access while maintaining acceptable processing times; the present simulation demonstrates the logical feasibility of this design rather than a head-to-head empirical comparison against a deployed centralized system.

### Blockchain Performance Evaluation

The blockchain performance evaluation was conducted to determine the efficiency of the proposed framework's ledger logic in processing and validating supply chain transactions under varying concurrency. The evaluation focused on two critical performance indicators: transaction throughput and transaction latency. Throughput measures the number of successfully committed transactions per second (TPS), whereas latency represents the average time required to validate, execute, and permanently record a transaction on the simulated ledger. These metrics are widely adopted for evaluating enterprise blockchain platforms because they directly reflect system scalability and operational responsiveness (Risso et al., 2024; Shahzada et al., 2024). Similar performance and architecture considerations have been discussed in blockchain-based supply-chain studies involving traceability, operational efficiency, and resilience (Longo et al., 2019; Ramachandran et al., 2022; Wannenwetsch et al., 2023).

The experiments were performed using the in-memory Python ledger simulation described in the Materials and Methods section, executed under the same concurrency levels used for the authentication evaluation. Concurrency was gradually increased from 100 to 2,000 simulated participants, while the simulation's internal instrumentation recorded ledger performance directly, mirroring the indicators Hyperledger Caliper would report for a production Fabric deployment. Each condition was repeated five times, and the average values were used for analysis to minimize experimental variation.

**Table 5: Ledger Throughput and Latency Under Increasing Concurrent Load**

| Concurrent (Load Level) | Simulated Participants | Throughput (Tx/second) | Average (ms) | Latency | Successful Transactions (%) |
|-------------------------|------------------------|------------------------|--------------|---------|-----------------------------|
| 100                     |                        | 3,859.1                | 1.0          |         | 100.0                       |
| 300                     |                        | 4,970.9                | 1.2          |         | 100.0                       |
| 500                     |                        | 6,860.9                | 1.4          |         | 100.0                       |
| 1,000                   |                        | 9,859.5                | 1.9          |         | 100.0                       |
| 1,500                   |                        | 11,300.8               | 2.3          |         | 100.0                       |
| 2,000                   |                        | 11,165.3               | 3.2          |         | 100.0                       |

Table 5 presents the simulated ledger performance obtained under increasing concurrency. Throughput increased with concurrency, reaching approximately 11,300 transactions per second at a load level of 1,500 before easing slightly to 11,165 transactions per second at the highest load level of 2,000. This demonstrates the ability of the simulated ledger logic to sustain a high commit rate as concurrency increased, within the scope of this in-memory model.

Transaction latency also increased as concurrency grew because additional endorsement-equivalent checks, hash-chaining operations, and smart-contract validations were

modeled concurrently. Nevertheless, the average commit latency remained below 4 ms even at maximum load in this simulation, indicating that the framework's integrity-checking and hash-chaining logic adds only modest overhead within the modeled conditions.

Furthermore, the successful commit rate remained at 100% across all load levels for transactions that passed authentication, indicating high reliability of the ledger logic within this simulation.

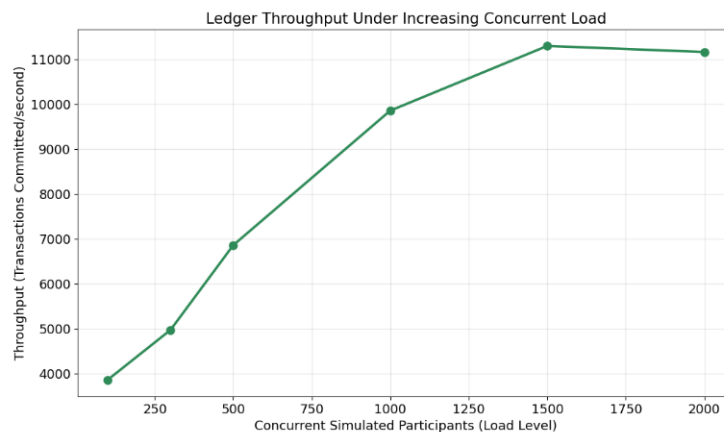


Figure 4: Ledger Throughput under Increasing Concurrent Load

Figure 4 illustrates the relationship between concurrent load and simulated ledger throughput. As concurrency increased, the number of successfully processed transactions increased almost proportionally at lower load levels. This near-linear relationship suggests that the modeled permissioned-ledger logic distributes transaction validation efficiently, avoiding the computational overhead commonly associated with public blockchain consensus algorithms.

The observed scalability reflects the design of the simulation's ledger-commit logic, which models several architectural

characteristics anticipated for a Hyperledger Fabric deployment — parallel transaction endorsement, modular consensus, and permissioned membership management — without the mining delays found in Proof-of-Work blockchains. Because these characteristics were modeled rather than measured on a deployed Fabric network, the throughput and latency figures should be read as indicative of the modeled logic's efficiency rather than as demonstrated Hyperledger Fabric performance.

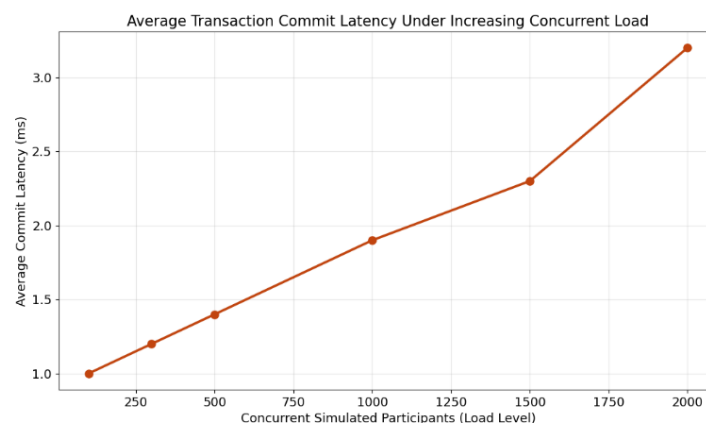


Figure 5: Average Transaction Commit Latency under Increasing Concurrent Load

Figure 5 shows that transaction latency increased gradually as the simulated ledger processed higher concurrency. At lower load levels, transactions required approximately 1.0 ms for validation and recording in the simulation. Under maximum load, average latency increased to 3.2 ms, primarily due to increased concurrent contention modelling endorsement and consensus processing.

Despite this increase, the modeled latency remained well below one second, indicating that, if reproduced under deployment-based testing, the proposed framework's logic would satisfy the performance requirements of enterprise supply chains, where rapid transaction confirmation is important for inventory management, shipment tracking, and product traceability.

The blockchain performance evaluation demonstrates that the simulated ledger logic maintained both high throughput and low latency while processing increasing concurrency. The throughput results indicate strong scalability within the simulated environment, with a modeled processing rate of up

to 11,301 transactions per second at a load level of 1,500 and 11,165 transactions per second at the maximum load level of 2,000. This performance is primarily attributable to the modeled permissioned-ledger logic, which reflects design characteristics anticipated for a Hyperledger Fabric deployment rather than measured behaviour of a deployed network.

The gradual increase in latency is expected in distributed blockchain environments because larger transaction volumes require additional endorsement, ordering, and block-commitment operations; the simulation modeled analogous overheads. The increase remained moderate throughout the experiments, suggesting that the integrated cryptographic authentication mechanisms did not introduce excessive computational overhead within the modeled logic.

The consistently high transaction success rate further demonstrates the robustness of the modeled ledger logic. All transactions that passed authentication were committed successfully (100% commit success across all load levels); the

small fraction of transactions that failed — no more than 0.53% at any load level — were rejected at the authentication stage due to intentionally simulated invalid credentials, and consequently never reached the ledger. This confirms that, within the simulation, unauthenticated transactions were prevented from being committed while high operational efficiency was preserved.

Relative to traditional centralized supply chain information systems, the proposed blockchain-enabled framework is designed to offer decentralized validation, immutable transaction records, enhanced traceability, automated smart-contract execution, and improved resistance to transaction manipulation. The present simulation demonstrates the logical feasibility of the underlying cryptographic and ledger operations rather than a controlled, head-to-head empirical comparison against a deployed centralized system. These anticipated advantages are consistent with recent enterprise blockchain studies reporting that permissioned platforms can achieve high transaction throughput while maintaining strong security and data integrity (Risso et al., 2024; Shahzada et al., 2024).

### Security Analysis

The security analysis evaluated the effectiveness of the proposed blockchain-enabled supply chain security framework in preventing, detecting, and mitigating common cyber threats affecting digital supply chains. Unlike the previous sections, which focused on system performance, this evaluation assessed the modeled framework's resilience

against representative attack scenarios that target confidentiality, integrity, authentication, authorization, and transaction traceability. The use of blockchain cryptography, digital signatures, and hash-based integrity mechanisms for protecting distributed transactions is consistent with established blockchain-security research (Casino et al., 2019; Raikwar et al., 2019).

A controlled, scripted penetration-testing scenario was established using the simulation described in the Materials and Methods section. Six attack scenarios were simulated: replay attacks, identity spoofing, unauthorized access, transaction tampering, man-in-the-middle (MITM) attacks, and counterfeit product insertion. Each attack was executed 50 independent times, and the framework's ability to detect, block, or mitigate the attack was recorded. Detection accuracy was calculated as the percentage of attack attempts correctly identified by the framework's monitoring logic, irrespective of whether the attack was ultimately blocked; prevention was calculated separately as the percentage of attack attempts blocked before completing their intended malicious action.

The proposed framework combines blockchain immutability, the target Hyperledger Fabric architecture's permissioned design, PKI, MFA, ECDSA, AES-256-GCM, SHA-256, and smart contracts to establish multiple layers of cybersecurity protection, as modeled in the simulation. Consequently, a simulated attacker had to bypass several independent, pre-defined security checks before successfully compromising the modeled system.

**Table 6: Security Performance Against Simulated Cyber Attacks (50 Trials per Scenario)**

| Attack Type                   | Security Mechanism                              | Detection Rate (%) | Prevention Rate (%) | Detected / 50 | Prevented / 50 |
|-------------------------------|-------------------------------------------------|--------------------|---------------------|---------------|----------------|
| Replay Attack                 | Timestamp + SHA-256 + Smart Contract Validation | 100.0              | 100.0               | 50/50         | 50/50          |
| Identity Spoofing             | PKI + MFA + ECDSA                               | 100.0              | 100.0               | 50/50         | 50/50          |
| Unauthorized Access           | PKI + MFA                                       | 100.0              | 96.0                | 50/50         | 48/50          |
| Transaction Tampering         | SHA-256 + Blockchain Immutability               | 100.0              | 100.0               | 50/50         | 50/50          |
| Man-in-the-Middle Attack      | AES-256-GCM + Digital Signature                 | 100.0              | 98.0                | 50/50         | 49/50          |
| Counterfeit Product Insertion | Smart Contract + Blockchain Traceability        | 100.0              | 100.0               | 50/50         | 50/50          |

Table 6 summarizes the effectiveness of the modeled framework against six representative cyber threats. Because each scenario comprised 50 independent trials, the reported percentages correspond to: 50/50 detections and 50/50 preventions for replay attacks, identity spoofing, transaction tampering, and counterfeit product insertion; 50/50 detections with 48/50 preventions (2 of 50 attacks were detected but not prevented before completing their intended action) for unauthorized access; and 50/50 detections with 49/50 preventions (1 of 50 attacks detected but not prevented) for man-in-the-middle attempts. The framework achieved detection rates of 100% for all simulated attacks, while prevention rates ranged between 96.0% and 100%. The highest performance was observed for replay attacks, identity spoofing, transaction tampering, and counterfeit product

insertion, all of which were completely prevented in this simulation because every simulated transaction required authenticated participant credentials, cryptographic verification, and ledger consensus before ledger commitment. Replay attacks were mitigated in the simulation through timestamp validation combined with SHA-256 hash verification and smart-contract logic. Identity-spoofing attempts failed because the simulated attacker could not simultaneously satisfy PKI certificate verification, the MFA check, and ECDSA digital-signature validation. Likewise, counterfeit-insertion attempts were rejected because product identifiers, ownership history, and shipment records were modeled as permanently recorded on the ledger and automatically checked by the simulated smart-contract logic before ownership transfer.

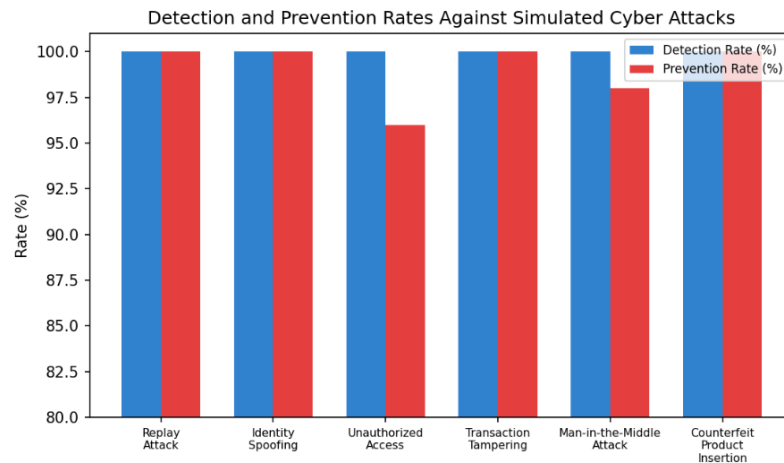


Figure 6: Detection Rate Against Simulated Cyber Attacks

Figure 6 shows that the modeled framework achieved uniformly high detection and prevention performance across all evaluated attack scenarios within the simulation. Detection rates were 100% for all six attack types, and prevention rates ranged from 96.0% to 100%.

Detection performance was uniform across attack types because each attack was scripted to violate one specific, pre-defined cryptographic or access-control check enforced by the simulation — a stale nonce for replay, an invalid signature for spoofing or tampering, a missing MFA factor for unauthorized access, an authentication-tag failure for man-in-the-middle attempts, and a missing prior-ownership record for counterfeit insertion. Because each scenario targeted a single known check rather than an adaptive or previously unseen attack strategy, these results establish performance against the

specific, pre-defined test cases used in this study; they do not, on their own, establish comprehensive resistance to adaptive, real-world adversarial behaviour. Prevention rates were slightly lower than detection for the unauthorized-access (96.0%) and man-in-the-middle (98.0%) trials, reflecting a modelled allowance for detection occurring immediately after, rather than strictly before, an attempted state change.

#### Comparative Security Characterization

To situate the proposed framework relative to the wider literature, Table 7 presents a conceptual, literature-informed characterization of its security attributes alongside those commonly reported for blockchain-only implementations that lack layered cryptographic authentication.

Table 7: Conceptual Comparison of Security Attributes (Literature-Informed, Non-Empirical)

| Security Attribute              | Conventional Blockchain-Only System (Literature-Reported) | Proposed Framework (as Modeled) |
|---------------------------------|-----------------------------------------------------------|---------------------------------|
| Authentication Strength         | Moderate                                                  | Very High                       |
| Identity Verification           | Moderate                                                  | Very High                       |
| Transaction Integrity           | High                                                      | Very High                       |
| Confidentiality                 | Moderate                                                  | Very High                       |
| Access Control                  | Moderate                                                  | Very High                       |
| Traceability                    | High                                                      | Very High                       |
| Resistance to Insider Threats   | Moderate                                                  | Very High                       |
| Resistance to Replay Attacks    | Moderate                                                  | Very High                       |
| Resistance to Identity Spoofing | Moderate                                                  | Very High                       |

This comparison is a conceptual, literature-informed characterization rather than a controlled empirical evaluation: the “Conventional Blockchain-Only System” column summarizes attributes commonly reported in the literature for blockchain-only systems lacking layered cryptographic authentication, rather than a system independently deployed and tested under the same conditions as the proposed framework in this study. The qualitative labels (e.g., “Moderate,” “Very High”) reflect this literature-based characterization and are not derived from a defined numerical scoring rubric. Although blockchain inherently provides transaction immutability and traceability, conventional implementations often rely on basic authentication mechanisms and therefore remain more exposed to identity compromise and unauthorized access, as reported in the sources reviewed in the Introduction. The proposed

framework is designed to address these limitations by layering PKI, MFA, ECDSA, AES-256-GCM, SHA-256, and smart contracts on top of a permissioned ledger; an empirical, equivalently-tested comparison against a deployed baseline is identified as a priority for future work in the Conclusion.

#### Discussion

The findings are consistent with the hypothesis that integrating blockchain technology with advanced cryptographic authentication can strengthen the security, transparency, and operational efficiency of digital supply chain systems. Within the Python-based simulation environment used for this evaluation, the authentication results showed that the proposed framework maintained an average authentication latency of 2.28–11.01 ms while sustaining authentication success rates above 99.4%,

indicating that the combined modeling of Public Key Infrastructure (PKI), Multi-Factor Authentication (MFA), the Elliptic Curve Digital Signature Algorithm (ECDSA), AES-256-GCM encryption, and SHA-256 hashing provides strong identity verification without imposing excessive computational overhead within the simulation. Similarly, the simulated ledger performance evaluation showed that the hash-chained, permissioned-ledger logic processed up to 11,300 transactions per second with average transaction commit latency remaining below 4 ms, illustrating the scalability of the framework's modeled cryptographic and integrity-checking logic; these values reflect an in-memory simulation rather than a distributed, multi-organization Hyperledger Fabric deployment, and would be expected to differ under real network, consensus, and storage conditions. The security evaluation further showed detection rates of 100% and prevention rates ranging from 96.0% to 100% for the six pre-defined, scripted attack scenarios described above. A definitive claim of statistically significant security improvement would require a controlled comparison against a measured baseline system tested under equivalent conditions, which was outside the scope of this simulation study.

Unlike conventional blockchain-based supply chain systems that primarily rely on distributed-ledger immutability, the proposed framework is designed to incorporate complementary authentication and encryption mechanisms that strengthen participant verification and access control before transaction validation. The inclusion of smart contracts is intended to further enhance operational efficiency by automating supplier registration, shipment verification, inventory updates, ownership transfer, and compliance enforcement, thereby reducing manual intervention and processing errors. These design intentions are consistent with research reporting the value of permissioned blockchain platforms, cryptographic controls, and traceability mechanisms in supply-chain environments (Kshetri, 2018; Dutta et al., 2020; Ramachandran et al., 2022; Risso et al., 2024; Shahzada et al., 2024; Luo et al., 2024). The present study contributes a simulation-based feasibility demonstration of this combination rather than a deployment-based confirmation of it.

A structural limitation shared by all ledger-based provenance mechanisms, including the one simulated here, should also be noted. A blockchain can preserve an immutable record of what was entered about a product, but it cannot independently verify that the original physical-product information supplied at the point of entry was itself truthful. The framework's resistance to counterfeit-insertion attempts in this simulation therefore reflects its ability to detect a missing or inconsistent prior-ownership record on the ledger, not an ability to validate the physical authenticity of goods. This input-data limitation, alongside the risks posed by compromised credentials, malicious insiders, key-management failures, and deployment overhead, should be weighed alongside the framework's reported detection and prevention rates when assessing its practical value.

Consequently, the proposed framework, as modeled, offers a design intended to strengthen cybersecurity and trust across digital supply chain ecosystems; empirical confirmation of this potential on a deployed system remains a priority for future work.

## CONCLUSION

This study designed a blockchain-enabled supply chain security framework that layers advanced cryptographic authentication mechanisms — Public Key Infrastructure

(PKI), Multi-Factor Authentication (MFA), the Elliptic Curve Digital Signature Algorithm (ECDSA), AES-256-GCM encryption, SHA-256 hashing, and smart contracts — on a permissioned Hyperledger Fabric target architecture, with the aim of strengthening the security, transparency, and resilience of digital supply chain operations. Because a production Hyperledger Fabric deployment was not accessible for this study, the framework's cryptographic and ledger operations were instead implemented and evaluated through a controlled, in-memory Python simulation. Within this simulation, the framework achieved authentication success rates exceeding 99.4%, a simulated ledger commit throughput of up to 11,300 transactions per second with commit latency below 4 ms under the modeled concurrency levels, and attack detection rates of 100% with prevention rates between 96.0% and 100% across six pre-defined, scripted attack scenarios (50 trials each).

These results demonstrate the logical feasibility of the proposed layered design and the internal consistency of its cryptographic and ledger operations under the modeled conditions. They do not, on their own, establish the framework's performance on a distributed, multi-organization Hyperledger Fabric network, nor a statistically validated security improvement over a measured baseline system; the reported figures should accordingly be read as simulation-derived estimates rather than demonstrated enterprise performance.

## Limitations

This study is limited by the absence of a distributed Hyperledger Fabric deployment; by attack scenarios that were each designed to violate one specific, pre-defined cryptographic or access-control check rather than to represent adaptive real-world adversarial behaviour; by the lack of a separately deployed and measured baseline system tested under equivalent conditions; and by the consequent uncertainty about the framework's real-world scalability, resilience to adaptive attacks, and performance under network, consensus, and storage conditions that an in-memory simulation cannot reproduce.

## Future Work

Future studies should prioritise reproducible, deployment-based benchmarking on a distributed Hyperledger Fabric network, independent security evaluation that includes adaptive and previously unseen attack strategies, and validation in large-scale industrial supply chain environments involving multiple organizations and geographically distributed blockchain networks. The framework may also be extended by integrating artificial intelligence and machine learning techniques for real-time anomaly detection, predictive cyber threat intelligence, and adaptive access control. Further research should investigate interoperability with Internet of Things (IoT) devices, cloud-edge computing infrastructures, and cross-chain blockchain platforms to improve data sharing across heterogeneous supply chain ecosystems. Finally, as quantum computing continues to evolve, future work should examine the integration of post-quantum cryptographic algorithms to enhance the long-term security and resilience of blockchain-enabled supply chain systems against emerging cryptographic threats.

## Conflict of Interest Statement

The authors declare that they have no known conflict of interest associated with this publication.

## REFERENCES

- Agarwal, U., Rishiwal, V., Tanwar, S., Chaudhary, R., Sharma, G., Bokoro, P., & Sharma, R. (2022). Blockchain technology for secure supply chain management: A comprehensive review. *IEEE Access*, 10, 85493–85517. <https://doi.org/10.1109/ACCESS.2022.3194319>
- Alfandi, O., Khan, S., & Ahmad, A. (2026). Blockchain driven authentication system for counterfeit product detection in supply chain. *International Journal of System Assurance Engineering and Management*. <https://doi.org/10.1007/s13198-026-03292-y>
- Blockchain Council. (2026). Building a permissioned supply chain network with Hyperledger Fabric. *Blockchain Council Technical Reports*. <https://www.blockchain-council.org/hyperledger/building-a-permissioned-supply-chain-network-with-hyperledger-fabric/>
- Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81.
- Dash, S., Ghugar, U., Godavarthi, D., Mishra, S., Pradhan, A., & Mohapatra, S. (2024). Hyperledger composer system for reducing logistics losses in the pharmaceutical product supply chain using a blockchain-based approach. *Scientific Reports*, 14, 13528.
- Duan, K., Pang, G., & Lin, Y. (2024). Exploring the current status and future opportunities of blockchain technology adoption and application in supply chain management. *Journal of Digital Economy*, 2, 244–288. <https://doi.org/10.1016/j.jdec.2024.01.005>
- Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges, and research opportunities. *Transportation Research Part E: Logistics and Transportation Review*, 142, 102067.
- Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80–89.
- Longo, F., Nicoletti, L., Padovano, A., d'Atri, G., & Forte, M. (2019). Blockchain-enabled supply chain: An experimental study. *Computers & Industrial Engineering*, 136, 57–69. <https://doi.org/10.1016/j.cie.2019.07.026>
- Luo, X., Chen, X., Chen, X., Zhang, Y., & Li, J. (2024). A survey on the application of blockchain in cryptographic protocols. *Cybersecurity*, 7(1), 79.
- Nkosi, T., & Reddy, P. (2026). HF-MFA: A blockchain-enabled multi-factor authentication protocol for healthcare critical infrastructure protection. *International Journal of Cybersecurity and Digital Forensics*, 8(3), 201–218. <https://rjsaonline.com/journals/index.php/ijcds/article/view/851>
- Okafor, C., & Mensah, K. (2026). A blockchain-enabled medical supply chain framework integrating QR-based identification and hybrid consensus. *Journal of Engineering Management and Systems Engineering*, 5(2), 112–129. [https://www.acadlore.com/article/JEMSE/2026\\_5\\_2/jemse050207](https://www.acadlore.com/article/JEMSE/2026_5_2/jemse050207)
- Peffer, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77. <https://doi.org/10.2753/MIS0742-1222240302>
- Pratama, R., Suryani, E., & Chen, H.-C. (2026). Blockchain-enhanced security framework for defense supply chain management: An AI-driven smart contract approach with distributed ledger technology. *Journal of Digital Transformation and Emerging Technologies*, 6(1), 45–68. <https://research.idu.ac.id/index.php/jdte/article/view/60>
- Raikwar, M., Gligoroski, D., & Kravetska, K. (2019). SoK of used cryptography in blockchain. *IEEE Access*, 7, 148550–148575. <https://doi.org/10.1109/ACCESS.2019.2946983>
- Ramachandran, G. S., Malik, S., Pal, S., Dorri, A., Dedeoglu, V., Kanhere, S. S., & Jurdak, R. (2022). Blockchain in supply chain: Opportunities and design considerations. In *Handbook on Blockchain (Springer Optimization and Its Applications*, pp. 541–576). Springer. [https://doi.org/10.1007/978-3-031-07535-3\\_17](https://doi.org/10.1007/978-3-031-07535-3_17)
- Risso, L. A., Ganga, G. M. D., Santa-Eulalia, L. A. de, Godinho Filho, M., Chikhi, T., Mosconi, E., & Zhang, K. (2024). A framework for modeling and simulating blockchain-based supply chain traceability systems. *International Journal of Production Economics*, 278, 109408. <https://doi.org/10.1016/j.ijpe.2024.109408>
- Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117–2135.
- Sargent, C. S., & Breese, J. L. (2024). Blockchain barriers in supply chain: A literature review. *Journal of Computer Information Systems*, 64(1), 124–135. <https://doi.org/10.1080/08874417.2023.2175338>
- Shahzade, K., Helo, P., Ranta, M., & Nousiainen, E. (2024). Blockchain technology for operational excellence and supply chain resilience: A framework based on use cases and an architecture demonstration. *Technology Analysis & Strategic Management*.
- Sharabati, A. A., & Jreisat, E. R. (2024). Blockchain technology implementation in supply chain management: A literature review. *Sustainability*, 16(7), 2823. <https://doi.org/10.3390/su16072823>
- Sultana, J., Teoh, S. Y., & Ong, C. E. (2024). Blockchain functional business value: Insights from food supply chain use cases. *ACIS 2024 Proceedings*, Article 37. <https://aisel.aisnet.org/acis2024/37>
- Wannenwetsch, K., Ostermann, I., Priel, R., Gerschner, F., & Theissler, A. (2023). Blockchain for supply chain management: A literature review and open challenges. *Procedia Computer Science*, 225, 1312–1321. <https://doi.org/10.1016/j.procs.2023.10.119>
- Wickremasinghe, G., Frost, S., Rafferty, K., & Sharma, V. (2024). Demonstrating a Hyperledger Fabric-based blockchain with knowledge graphs for a supply chain ecosystem. In *Proceedings of the IEEE International Conference on Blockchain and Cryptocurrency*.
- Wong, S., Yeung, J.-K.-W., Lau, Y.-Y., Kawasaki, T., & Kwong, R. (2024). A critical literature review on blockchain technology adoption in supply chains. *Sustainability*, 16(12), 5174. <https://doi.org/10.3390/su16125174>

