

ARTICLE

Explainable AI (XAI)-Based Security Verification in Blockchain-Enabled Drug Supply Chains

Muammar Shahrear Famous^{1,2} , Samia Sayed^{1,2} , Rashed Mazumder¹ , Risala T. Khan¹ ,
M. Shamim Kaiser¹ , Mohammad Shahadat Hossain³ and Karl Andersson^{4,*}

¹Institute of Information Technology (IIT), Jahangirnagar University, Savar, Bangladesh

²Department of Mathematics, Natural Sciences and Data Processing, THM University of Applied Sciences, Friedberg, Germany

³Department of Computer Science & Engineering, University of Chittagong, Chattogram, Bangladesh

⁴Department of Computer Science, Electrical and Space Engineering, Luleå University of Technology, Skellefteå, Sweden

*Corresponding Author: Karl Andersson. Email: karl.andersson@ltu.se

Received: 28 April 2026; Accepted: 02 July 2026; Published: 28 September 2026

ABSTRACT: Counterfeit pharmaceuticals, fragmented data management, and the absence of transparent verification mechanisms continue to threaten the integrity of modern healthcare drug supply chains. Although blockchain-based traceability frameworks improve decentralization and auditability, existing approaches frequently lack formally verified authentication guarantees and interpretable security decision mechanisms. To address these limitations, this paper proposes a unified blockchain-enabled healthcare supply-chain framework integrating nonce-based cryptographic authentication, formal security verification, Solidity smart contracts, and SHAP-based explainable artificial intelligence (XAI). The proposed protocol employs elliptic-curve digital signatures, nonce-based challenge–response authentication, and blockchain validation mechanisms to ensure secure communication among manufacturers, distributors, pharmacies, and regulatory authorities. Formal verification using ProVerif under the Dolev–Yao adversarial model confirms secrecy, authentication, integrity, and replay-attack resistance properties, with no executable attack traces detected. A permissioned Ethereum test network and Python-based cryptographic simulation environment were implemented using Solidity, Web3.py, and Py-EVM to evaluate deployment feasibility. Additional deployment validation was performed through Ethereum Sepolia test-network execution and Mythril smart-contract security auditing. Experimental results demonstrate stable and scalable operational performance, achieving average transaction latency below 3 s, throughput performance comparable to recent healthcare blockchain systems reporting approximately 95–155 transactions per second, and average cryptographic signing time of 0.71 ms per transaction. Gas-consumption analysis reported a mean transaction cost of 182,345 gas units with low execution variance, while storage overhead exhibited near-linear scalability as transaction volume increased. Additional adversarial evaluation demonstrated resilient transaction-validation behavior under varying node participation and simulated communication disruptions. To improve interpretability and regulatory transparency, the framework integrates SHAP-based explainable verification capable of identifying the relative influence of signature validity, nonce freshness, blockchain confirmation, and integrity verification on transaction acceptance decisions. Ablation analysis additionally showed that the complete integrated framework achieved 96.8% security assurance, 94.5% interpretability, and 97.2% traceability performance, substantially outperforming partial configurations lacking blockchain, formal verification, or explainability modules. The principal contribution of this work lies in combining formally verified authentication, blockchain-enabled traceability, explainable security analytics, and deployment-oriented validation within a unified pharmaceutical supply-chain architecture suitable for secure, scalable, and regulation-aware healthcare environments.

KEYWORDS: XAI; blockchain; HSCM; cryptographic protocol design; formal security verification; smart contracts; replay attack detection; pharmaceutical traceability; explainable security; blockchain auditability

1 Introduction

The integrity of pharmaceutical supply chains has become a critical global healthcare concern due to the rapid growth of counterfeit medications, fragmented logistics infrastructures, and insufficient transparency across distributed stakeholders. Counterfeit and tampered pharmaceutical products not only generate major economic losses but also pose severe risks to patient safety, treatment reliability, and regulatory compliance. Modern healthcare drug supply chains involve multiple independent entities—including manufacturers, distributors, pharmacies, hospitals, and regulatory authorities—that continuously exchange sensitive transactional and logistical information throughout the drug lifecycle. Ensuring secure traceability and trustworthy verification across these heterogeneous participants therefore remains a fundamental requirement for modern healthcare systems. Nevertheless, conventional drug supply-chain management systems are largely centralized and depend on fragmented databases administered independently by different organizations. Such architectures introduce significant vulnerabilities, including reduced transparency, susceptibility to data tampering, delayed verification processes, limited interoperability, and the widespread circulation of counterfeit pharmaceutical products. Fig. 1 illustrates that incidents involving counterfeit drugs have shown a general upward trend across most regions, posing considerable risks to patient safety and healthcare reliability. Furthermore, traditional systems frequently struggle to provide real-time verification of drug provenance, making it difficult for regulators and healthcare providers to detect anomalies or identify unauthorized modifications to pharmaceutical products [1].

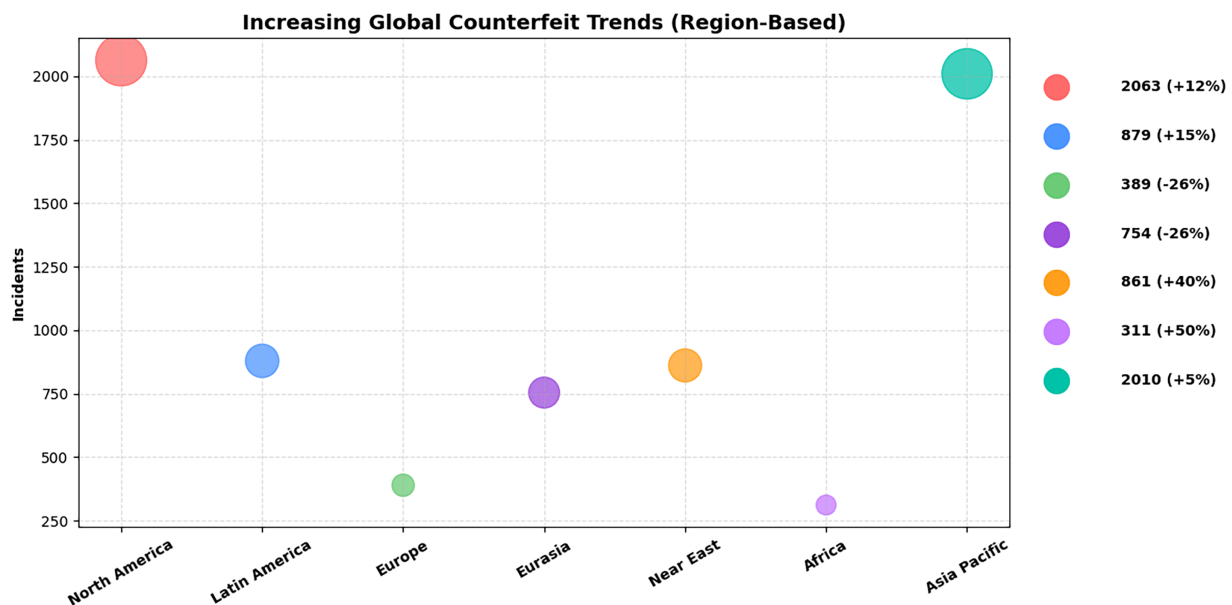


Figure 1: Global spread and growing occurrences of pharmaceutical counterfeiting across different time periods, supplemented by an analysis of trends observed across various regions. Source: <https://www.psi-inc.org/geographic-distribution>.

To overcome these limitations, recent research has increasingly explored blockchain technology as a mechanism for establishing decentralized, tamper-resistant, and auditable pharmaceutical supply-chain

infrastructures. Through distributed ledger technology, blockchain enables multiple stakeholders to record and verify transactions within a shared immutable environment where previously committed records cannot be altered without consensus [2]. Within pharmaceutical supply chains, blockchain can improve product provenance tracking, facilitate automated transaction validation using smart contracts, and strengthen trust among participating entities. However, blockchain technology alone cannot fully address the broader security and transparency challenges associated with healthcare supply-chain environments. Secure communication among distributed stakeholders still requires robust cryptographic authentication protocols capable of resisting replay attacks, impersonation attempts, unauthorized transaction modification, and malicious data injection [3]. Moreover, while blockchain provides immutable storage and decentralized verification, it does not inherently guarantee formally verified authentication correctness or interpretable decision transparency for regulators and healthcare authorities.

Beyond cryptographic protection and immutable transaction storage, healthcare stakeholders also require transparent and interpretable verification mechanisms capable of explaining why specific transactions are accepted, rejected, or flagged as suspicious. Existing cryptographic verification systems and formal protocol verification tools often provide mathematically rigorous security guarantees but produce outputs that are difficult for non-technical users to interpret. In healthcare environments, regulatory authorities, auditors, and supply-chain operators frequently require human-understandable reasoning to support compliance verification, anomaly investigation, and operational trust in automated security systems. To address these challenges, Explainable Artificial Intelligence (XAI) has emerged as an important mechanism for improving interpretability and transparency within intelligent decision-making systems. Integrating explainability with blockchain-based healthcare infrastructures can therefore improve auditability and strengthen stakeholder confidence in automated transaction-verification processes.

Despite recent advancements in blockchain-enabled healthcare security and explainable artificial intelligence, several important research gaps remain unresolved. Existing blockchain-based healthcare frameworks primarily focus on decentralized traceability and immutable record management but often lack formally verified authentication mechanisms capable of resisting replay and impersonation attacks. Similarly, many formal verification studies emphasize protocol correctness while providing limited interpretability regarding security-verification outcomes for healthcare stakeholders and regulators. In parallel, XAI approaches improve transparency in machine learning systems; however, most existing explainability solutions operate independently from immutable blockchain infrastructures and therefore lack tamper-resistant auditability and decentralized verification guarantees. Furthermore, only limited research has explored the unified integration of blockchain security, formal cryptographic verification, smart-contract-enabled traceability, and explainable transaction validation within a single pharmaceutical supply-chain architecture. These limitations motivate the need for a secure, interpretable, and formally verifiable framework capable of supporting trustworthy healthcare supply-chain operations.

To address these challenges, this study proposes a unified blockchain-enabled healthcare drug supply-chain framework integrating formally verified cryptographic authentication, decentralized blockchain traceability, Solidity smart contracts, and SHAP-based explainable security analytics. The proposed framework employs nonce-based challenge–response authentication, elliptic-curve digital signatures, and blockchain transaction validation mechanisms to establish secure communication among manufacturers, distributors, pharmacies, and regulatory authorities. Formal verification using ProVerif is applied to validate secrecy, authentication, and replay-attack resistance properties under the symbolic Dolev–Yao adversarial model, while SHAP-based explainability is integrated to provide interpretable reasoning for transaction verification outcomes. To evaluate practical feasibility beyond theoretical protocol design, the proposed

framework is implemented within a permissioned Ethereum-based prototype environment integrating smart contracts, cryptographic authentication, formal verification, and explainable transaction analysis.

1.1 Research Questions

Based on the identified limitations in existing healthcare security frameworks, this study investigates the following research questions:

- **RQ1:** Can formally verified blockchain protocols improve authentication security and replay-attack resistance in pharmaceutical supply chains?
- **RQ2:** Can SHAP-based explainability provide interpretable and auditable reasoning for blockchain transaction verification decisions?
- **RQ3:** Can the integration of blockchain, formal verification, and explainable AI maintain practical computational performance for real-world healthcare supply-chain operations?

The central hypothesis of this study is that integrating formally verified authentication protocols with blockchain-enabled traceability and SHAP-based explainability can simultaneously improve security, transparency, auditability, and operational trust within pharmaceutical supply-chain systems while maintaining practical computational overhead suitable for healthcare deployment environments.

A working prototype is developed using a Python-based cryptographic simulation together with a permissioned Ethereum testing environment to evaluate the practicality and scalability of the proposed framework. The experimental evaluation analyzes several key performance indicators, including transaction latency, throughput, gas consumption, storage overhead, fault tolerance, and cryptographic signing cost. The findings demonstrate that the proposed architecture can provide secure authentication, decentralized traceability, interpretable verification transparency, and efficient computational performance suitable for healthcare deployment scenarios. The principal technical and methodological contributions of this study are summarized in the following subsection.

1.2 Key Contributions

The major contributions of this study are summarized as follows:

- A formally verified nonce-based cryptographic authentication protocol is developed and analyzed using ProVerif to ensure secrecy, authentication, integrity, and replay-attack resistance under the symbolic Dolev–Yao adversarial model.
- A blockchain-enabled pharmaceutical supply-chain architecture is implemented using Solidity smart contracts and a permissioned Ethereum testing environment to provide decentralized traceability, immutable transaction logging, and secure drug-batch verification.
- A SHAP-based explainable verification module is integrated to provide interpretable reasoning for transaction validation and rejection decisions, thereby improving transparency, regulatory auditability, and stakeholder trust.
- Comprehensive experimental and deployment-oriented evaluation is conducted using simulated healthcare transaction workloads, ProVerif analysis, Solidity smart contracts, and Ethereum-based testing environments to assess transaction latency, throughput, gas consumption, storage scalability, fault tolerance, and explainability performance.

2 Related Work

2.1 Blockchain-Based Healthcare and Drug Supply Chains

Blockchain technology has emerged as a promising approach for improving transparency, integrity, and traceability in healthcare and pharmaceutical supply chains. Arslanoğlu and Karaköse [4] highlighted the importance of integrating blockchain with explainable and trustworthy healthcare infrastructures, although practical implementation remains limited. In pharmaceutical logistics, Rupa et al. [5] proposed a blockchain-based decentralized application integrated with AI-driven drug recommendation systems, but scalability and privacy concerns limited deployment feasibility. Abbas et al. [6] developed a blockchain-machine learning architecture for healthcare traceability, though the system relied heavily on simulations and lacked large-scale validation. Alsagheer et al. [7] introduced decentralized governance models without implementing a complete decentralized application.

Several studies concentrated on enhancing drug traceability and counterfeit prevention. Charles et al. [8] and Pathak et al. [9] improved supply-chain monitoring and transparency but lacked sufficient implementation-level validation. Ahmadi et al. [10] and Singh et al. [11] integrated IoT devices with blockchain-enabled healthcare logistics, although scalability and fault-tolerance limitations remained unresolved. Omar et al. [12] and Cui et al. [13] further strengthened traceability frameworks for pharmaceutical systems but encountered scalability and interoperability challenges. Amoozad Mahdiraji et al. [14] investigated drug traceability using the Pythagorean Fuzzy-Delphi method, though the absence of blockchain integration limited secure and decentralized verification capabilities. Kumar and Das [15] introduced RFID-assisted blockchain authentication mechanisms for healthcare logistics, though deployment complexity and operational overhead remained significant.

Recent works additionally explored AI-assisted blockchain ecosystems for healthcare security. Liu et al. [16] integrated AI, IoT, and blockchain to enhance intelligent healthcare operations, though the framework introduced coordination complexity and computational overhead. Crossland et al. [17] and Agrawal et al. [18] further emphasized scalability and privacy concerns in public blockchain healthcare systems.

Despite substantial progress, existing blockchain-enabled healthcare systems continue to encounter limitations associated with scalability, interoperability, deployment readiness, and decentralized identity management. These unresolved issues motivate the development of lightweight and practically deployable architectures capable of supporting secure and transparent pharmaceutical supply-chain operations.

2.2 Formal Verification and Cryptographic Security

Formal verification and cryptographic authentication have become essential for ensuring secure communication and trustworthy transaction validation within decentralized healthcare environments. Chen et al. [19] and Sayed et al. [20,21] proposed secure cryptographic healthcare architectures to strengthen resilience against cyber threats, although implementation-level validation remained limited. Altigani et al. [22] and Booher et al. [23] introduced polymorphic encryption mechanisms to improve protocol robustness; however, these approaches suffered from substantial computational cost and hardware dependency.

Identity-based and lattice-based cryptographic frameworks have also been widely investigated. Meng and Li [24] and Shim and An [25] proposed advanced authentication and encryption methods for secure communication, though increased computational complexity limited practical deployment. Simion [26] and Xie et al. [27] examined secure encryption architectures for decentralized environments, but large-scale real-world implementation remained insufficiently explored.

System-level security studies additionally highlighted implementation and scalability limitations. Kim [28] developed optimized cryptographic frameworks with strong theoretical guarantees but limited operational flexibility. Dashtizadeh et al. [29] and Debe et al. [30] proposed detection and monitoring systems without fully integrating decentralized applications. Musamih et al. [31,32] encountered challenges related to privacy preservation and data immutability. Mohit et al. [33] and Saindane et al. [34] reported performance inefficiencies and automation limitations, while Marbough et al. [35] and related studies [36] lacked sufficient usability and deployment analysis.

Additional research focused on interoperability and cloud-assisted secure infrastructures. Chang and Chen [37] identified significant interoperability gaps in healthcare blockchain systems, while Sahoo et al. [38] lacked smart-contract automation capabilities. Jamil et al. [39] and Pham et al. [40] proposed decentralized healthcare security solutions but did not provide realistic deployment validation. He and He [41] and Mani et al. [42] introduced cloud-assisted architectures affected by communication overhead and optimization inefficiencies. Xu et al. [43] concentrated on privacy enhancement while insufficiently addressing scalability concerns.

Collectively, these studies demonstrate that although formal verification and advanced cryptographic protocols strengthen healthcare system security, many frameworks still struggle with computational complexity, deployment overhead, interoperability, and real-world scalability.

2.3 Explainable AI and Blockchain-Based Auditing

Recent research has increasingly explored the integration of Explainable Artificial Intelligence (XAI) with blockchain technologies to improve transparency, accountability, and trustworthiness in intelligent healthcare systems. Sowjanya et al. [44] proposed a hybrid architecture combining Federated Learning (FL), XAI, and blockchain for IoT-enabled healthcare applications. While the framework improved decentralized trust and interpretability, it introduced high latency and computational overhead. Murthy and Shri [45] developed an XAI-Blockchain middleware utilizing smart contracts and lightweight communication protocols, though scalability and interoperability issues persisted.

Dutta et al. [46,47] integrated SHAP and LIME explainability techniques within blockchain healthcare systems to improve transparency in medical decision-making. However, the proposed frameworks increased architectural complexity and limited real-time deployment feasibility. Ali et al. [48] explored the combination of XAI and blockchain in metaverse healthcare systems, although privacy and trust mechanisms remained immature. Beyond healthcare, blockchain-backed explainability has been applied to infrastructure and industrial systems. Mavrogiorgos et al. [49] proposed explainable blockchain-driven policy systems for water management, while Njoku et al. [50] combined SHAP explainability with blockchain-enabled battery management systems. Wang et al. [51] introduced explainable semantic communication frameworks, and Rathod et al. [52] developed blockchain-secured XAI architectures for IoT critical infrastructures. Gadekallu et al. [53] further highlighted persistent transparency and interoperability gaps within Industry 5.0 ecosystems.

Security-focused explainability studies additionally demonstrated the importance of interpretable cybersecurity analytics. Hasan et al. [54,55] utilized SHAP-based explainability for fraud and anomaly detection within blockchain systems, though scalability and class imbalance remained unresolved. Kritika [56] addressed ransomware and DDoS detection using explainable deep-learning approaches, yet real-time robustness and adversarial resilience remained limited. Zhang et al. [57], Bonnet et al. [58], and Al Ghanmi and Bahsoon [59] investigated responsible AI practices and explainable smart contracts, though

healthcare-oriented deployment validation was still lacking. More recent discussions have considered AI-integrated blockchain intelligence. Bistarelli et al. [60] proposed a hybrid blockchain framework with limited experimental validation.

Ressi et al. [61] reviewed the integration of artificial intelligence and blockchain technologies, emphasizing how AI techniques can enhance blockchain scalability, consensus optimization, smart-contract execution, and decentralized security management. Their study examined machine learning, deep learning, natural language processing, and reinforcement learning approaches applied within blockchain infrastructures rather than functioning solely as external analytical components. The authors concluded that AI-enhanced blockchain systems can significantly improve operational efficiency, adaptive decision-making, and intelligent transaction management while also identifying future research opportunities in autonomous and self-optimizing distributed ledger architectures. This perspective further highlights the importance of integrating explainability and intelligent verification directly into blockchain-enabled healthcare systems.

2.4 Federated and Privacy-Preserving Learning

Federated and privacy-preserving learning techniques have gained substantial attention due to their ability to support collaborative intelligence without exposing sensitive healthcare data. Madupati et al. [62] proposed blockchain-audited federated learning pipelines for trustworthy healthcare analytics, although scalability and data-validation issues persisted. Pavlova et al. [63] introduced decentralized federated learning combined with secret-sharing mechanisms, but the framework incurred high training cost and computational overhead.

Mu et al. [64] addressed healthcare-data heterogeneity using causal learning integrated with blockchain technology, though communication overhead significantly affected efficiency. Kumar et al. [65] applied artificial intelligence for medical equipment supply chain optimization, but lacked blockchain-enabled traceability and privacy-preserving learning mechanisms. Korde et al. [66] and Potdukhe et al. [67] emphasized privacy preservation, ethics, and explainability within blockchain-enabled machine learning systems, while identifying the ongoing need for lightweight and scalable architectures.

Additional studies explored intelligent decentralized healthcare infrastructures. Chang and Chen [37], Jamil et al. [39], and Pham et al. [40] investigated decentralized healthcare data-sharing frameworks but lacked realistic deployment validation. He and He [41], Mani et al. [42], and Xu et al. [43] focused on privacy-preserving healthcare infrastructures, although scalability and optimization remained insufficiently addressed.

These studies collectively demonstrate that while federated learning significantly enhances healthcare privacy preservation, integrating federated intelligence with blockchain auditing, explainability, and lightweight deployment architectures remains an open challenge.

2.5 Research Gaps and Motivation

A comprehensive review of the literature reveals several critical limitations that continue to hinder the real-world deployment of existing healthcare security frameworks:

- Existing systems lack a unified integration of Explainable AI, Federated Learning, and Blockchain, resulting in either explainable but insecure models or secure but non-interpretable systems.
- Most proposed frameworks suffer from scalability issues and insufficient real-world deployment validation, relying primarily on simulations or constrained datasets.
- Advanced cryptographic and AI-driven mechanisms often introduce substantial computational overhead and architectural complexity, thereby limiting practical adoption in healthcare environments.

The principal limitations identified across recent studies are summarized in [Table 1](#). Motivated by these challenges, the present study introduces a unified framework integrating Explainable AI, Federated Learning, blockchain-based auditing, and formally verified cryptographic security. In contrast to existing approaches, the proposed architecture simultaneously ensures interpretability, privacy preservation, tamper-resistant auditability, and lightweight operational scalability. Furthermore, the framework incorporates SHAP-based explainability alongside blockchain-backed verification trails to provide transparent and trustworthy decision support within pharmaceutical supply-chain environments. By addressing the identified limitations in security, scalability, explainability, and deployment feasibility, the proposed system aims to provide a practical and reliable solution for secure healthcare logistics and pharmaceutical traceability systems.

Table 1: Compilation of the latest and most pertinent studies, summarizing their respective objectives and identified limitations.

Reference	Objective	Limitation
[5] (2025)	Develop blockchain-based DApp with AI drug recommendation	Scalability and privacy concerns in public blockchain
[44] (2025)	Integrate FL, XAI, and blockchain for IoT healthcare security	High latency and computational overhead
[45] (2024)	Develop XAI-Blockchain middleware with smart contracts	Poor scalability and interoperability issues
[46] (2024)	Apply SHAP-based explainability in blockchain healthcare	Complex architecture with limited real-time usability
[48] (2023)	Combine XAI and blockchain in metaverse healthcare	Weak privacy and immature trust mechanisms
[55] (2024)	Detect anomalies in blockchain using XAI models	Scalability limitations in large networks
[59] (2024)	Design explainable smart contracts for transparency	Lacks healthcare-specific deployment validation
[62] (2025)	Build blockchain-audited federated learning pipelines	Data validation gaps and scalability constraints
[63] (2025)	Propose decentralized FL with secure sharing	High training cost and limited deployment feasibility
[64] (2024)	Use causal XAI with blockchain for medical imaging	Communication overhead and inefficiency

3 Methodology

The proposed framework brings together blockchain infrastructure and a cryptographic authentication protocol to establish secure drug traceability across the healthcare supply chain. The system involves four primary stakeholders: Manufacturer (M), Distributor (D), Pharmacy/Hospital (P), and Regulatory Authority (R). Each entity engages with a shared blockchain network where drug transactions and verification events are captured as immutable records. Blockchain provides tamper resistance, while the cryptographic protocol ensures secure authentication and communication among all participating parties.

Fig. 2 presents the proposed system architecture. As depicted in Fig. 1, manufacturers register drug batches on the blockchain using cryptographic identifiers, and distributors along with pharmacies validate transactions through the secure protocol before recording supply chain events. The regulatory authority monitors these transactions on an ongoing basis to verify compliance and flag any suspicious activity. This architecture guarantees end-to-end traceability and accountability throughout the entire pharmaceutical lifecycle. Each participant engages with the blockchain network through authenticated transactions governed by smart contracts, while sensitive operational data is handled through off-chain storage.

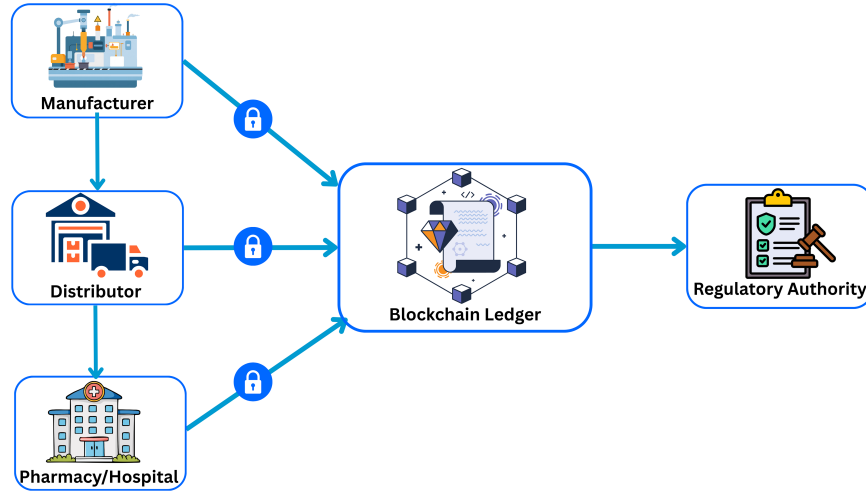


Figure 2: This figure presents the architecture of the proposed blockchain-integrated healthcare drug supply chain system. It depicts the manner in which participating stakeholders engage with the blockchain ledger by means of secure cryptographic authentication and verification mechanisms, collectively working to uphold transparency and data integrity throughout the chain.

3.1 System Model and Problem Formulation

The proposed healthcare drug supply-chain framework consists of four primary entities: manufacturer (M), distributor (D), pharmacy (P), and blockchain network (B). Each participant communicates through authenticated blockchain transactions secured using nonce-based cryptographic verification and digital signatures.

Let T_i represent a blockchain transaction associated with drug batch i . Each transaction contains transaction metadata, participant identity, timestamp, nonce value, and digital signature information:

$$T_i = \{ID_i, N_i, TS_i, Sig_i, H_i\}$$

where N_i denotes the nonce used for replay-attack prevention, TS_i represents the timestamp, Sig_i denotes the elliptic-curve digital signature, and H_i represents the cryptographic hash of the transaction payload. The mathematical notation used in the proposed framework is shown in Table 2.

The adversarial model assumes the presence of an attacker $\mathcal{A}$ operating under the Dolev-Yao threat model. The attacker is capable of intercepting, replaying, modifying, and injecting messages into the communication channel:

$$\mathcal{A} = \{Intercept, Replay, Modify, Inject\}$$

while cryptographic primitives are assumed to be computationally secure and non-breakable. The objective of the proposed framework is to minimize computational overhead while maximizing transaction security, traceability, and explainability. The optimization objective can be expressed as:

$$\min(L_t + C_g + S_o)$$

where L_t represents transaction latency, C_g denotes blockchain gas consumption, and S_o indicates storage overhead. Simultaneously, the framework aims to maximize authentication integrity and explainable verification transparency.

Table 2: Mathematical notation used in the proposed framework.

Symbol	Description
M	Manufacturer node
D	Distributor node
P	Pharmacy node
B	Blockchain network
T_i	Blockchain transaction
N_i	Nonce value
TS_i	Timestamp
Sig_i	Digital signature
H_i	Transaction hash
$\mathcal{A}$	Adversarial entity
L_t	Transaction latency
C_g	Gas consumption
S_o	Storage overhead

3.2 Threat Model and Security Assumptions

The proposed system assumes the presence of an adversary capable of intercepting network communications, attempting impersonation attacks, or manipulating transaction messages. In an open supply chain environment, malicious actors may attempt to inject counterfeit drug data or impersonate legitimate stakeholders to disrupt drug traceability.

To mitigate these threats, the protocol assumes secure cryptographic primitives including hash functions and digital signatures. The adversary follows the widely accepted Dolev–Yao attacker model, where attackers can observe and modify messages but cannot break strong cryptographic functions. The integrity of blockchain data ensures that once transactions are validated and recorded, they cannot be altered. The security of the cryptographic hashing function is defined as:

$$h = H(m),$$

where $H(\cdot)$ denotes a cryptographically secure hash function, and m represents the input message corresponding to the drug batch data. Fig. 3 illustrates the threat environment where malicious actors attempt to manipulate supply chain messages before they reach legitimate stakeholders.

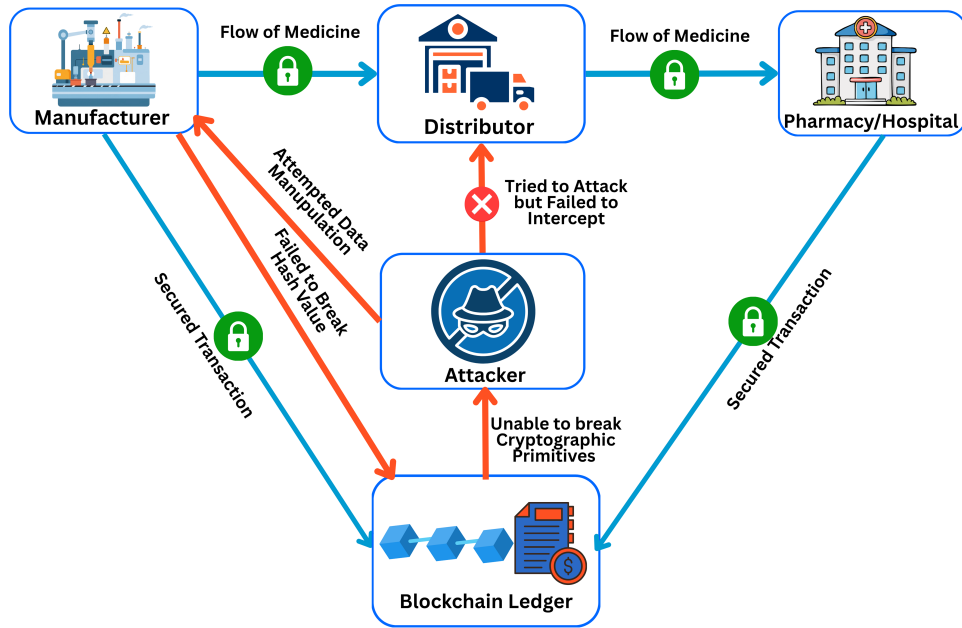


Figure 3: If an attacker attempts to intercept or tamper with communication messages exchanged between stakeholders, the immutability of blockchain records combined with robust cryptographic verification mechanisms renders such attacks unsuccessful.

3.3 Design of the Cryptographic Security Protocol

The proposed protocol establishes secure authentication and transaction validation among stakeholders in the drug supply chain. Each participant possesses a public-private key pair used for signing and verifying drug transactions before they are committed to the blockchain network. The protocol ensures three major security objectives: authentication, confidentiality, and integrity. A secure session key is generated between communicating entities using asymmetric cryptography. The transaction verification process ensures that only authorized entities can initiate supply chain updates.

Algorithm 1 describes the cryptographic protocol used for authenticating drug batch transactions before they are written to the blockchain. The process ensures that only authorized manufacturers can generate valid supply chain records and prevents unauthorized modification of drug information.

Algorithm 1: Secure drug batch verification and blockchain logging

Input: Drug batch data DB , manufacturer's secret key SK_M , public key PK_M

Output: Validated and recorded blockchain transaction

- 1 Manufacturer generates batch ID;
 - 2 Compute hash value $H(DB)$;
 - 3 Create digital signature $S \leftarrow \text{Sign}(SK_M, H(DB))$;
 - 4 Send (DB, S) to distributor;
 - 5 Distributor verifies signature using PK_M ;
 - 6 Verify that $BatchID$ is not already registered;
 - 7 **if signature is valid then**
 - 8 Create transaction record T ;
 - 9 Submit T to blockchain network;
-

(Continued)

Algorithm 1 (continued)

```

10  Blockchain validates and stores transaction;
11  else
12  Reject transaction;

```

Cryptographic Protocol Message Flow

To ensure secure authentication and transaction validation among stakeholders, the proposed framework defines an explicit cryptographic protocol consisting of seven message exchanges. The protocol is designed to establish trust between supply chain participants while ensuring confidentiality, integrity, and resistance against replay or impersonation attacks. Explicit protocol message definitions are commonly used in security protocol research to enable formal modeling and verification.

The protocol involves four entities: Manufacturer (M), Distributor (D), Pharmacy (P), and the Blockchain Network (BC). Each entity possesses a public–private key pair used for encryption and digital signature generation. Let PK_x and SK_x represent the public and private keys of entity x , respectively. A cryptographic hash function is used to ensure data integrity, defined as $H(x) = \text{SHA256}(x)$. Fig. 4 illustrates the proposed message exchange process for secure authentication and drug batch verification. The protocol consists of the following message sequence:

$M1: M \rightarrow D : \{ID_M, BatchID, Nonce_M\}_{PK_D}$
 $M2: D \rightarrow M : \{Nonce_M, Nonce_D\}_{PK_M}$
 $M3: M \rightarrow D : \text{Sign}_{SK_M}(BatchID \parallel Nonce_D)$
 $M4: D \rightarrow BC : \{BatchID, Signature_M\}$
 $M5: BC \rightarrow P : \text{Verified}(BatchID)$
 $M6: P \rightarrow BC : \text{ConfirmReceipt}(BatchID)$
 $M7: BC \rightarrow All : \text{LedgerUpdate}(BatchID)$

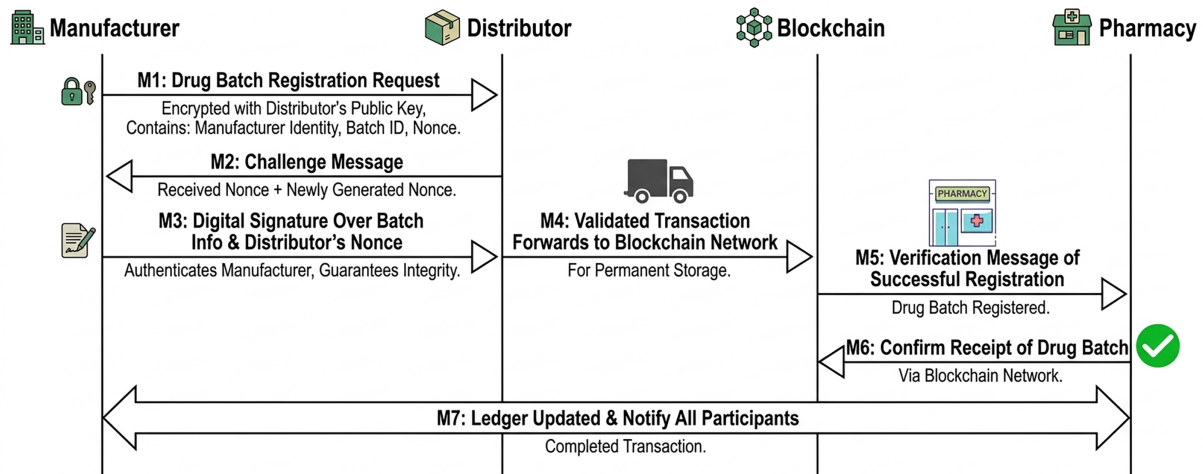


Figure 4: Formal nonce-based message-flow sequence of the proposed blockchain authentication protocol among manufacturer, distributor, pharmacy, and blockchain entities. The protocol integrates nonce exchange, digital signatures, transaction verification, and blockchain commitment to ensure authentication, integrity, and replay-attack resistance.

The authentication process begins when the manufacturer initiates communication by sending a drug batch registration request to the distributor, encrypted using the distributor's public key (M1). This message contains the manufacturer identity, batch identifier, and a nonce value to prevent replay attacks. The distributor responds with a challenge message containing the received nonce and a newly generated nonce (M2), ensuring mutual authentication between both parties.

After validating the challenge message, the manufacturer generates a digital signature over the batch information and the distributor's nonce (M3). This signature confirms the authenticity of the manufacturer and guarantees the integrity of the transmitted batch data. The distributor verifies the signature and forwards the validated transaction to the blockchain network for permanent storage (M4). Once the blockchain validates the transaction, a verification message is sent to the pharmacy indicating that the drug batch has been successfully registered (M5). The pharmacy then confirms receipt of the drug batch through the blockchain network (M6), after which the blockchain updates the global ledger and notifies all participants of the completed transaction (M7). This process ensures end-to-end traceability and secure verification across the pharmaceutical supply chain.

The protocol ensures multiple security properties, including mutual authentication, message integrity, replay attack resistance, and non-repudiation of drug registration events.

3.4 Formal Modeling of the Protocol

To guarantee protocol correctness, the authentication protocol is formally modeled using symbolic protocol representation. Each message exchange between entities is represented as a state transition, enabling formal verification tools to analyze protocol security properties. Let M , D , and P denote Manufacturer, Distributor, and Pharmacy, respectively. The protocol message exchange can be defined as:

$$\begin{aligned} M &\rightarrow D : \{ID_M, \text{BatchID}, H(DB)\}_{SK_M} \\ D &\rightarrow P : \{\text{BatchID}, H(DB)\}_{PK_P} \end{aligned}$$

These equations represent the secure transmission of drug batch identifiers and associated hashes using cryptographic keys. The formal representation ensures that the protocol structure can be analyzed for vulnerabilities such as replay attacks and message forgery. The protocol is modeled using a symbolic representation suitable for automated security verification tools such as ProVerif.

3.5 Computational and Communication Complexity Analysis

The computational overhead of the proposed protocol primarily depends on elliptic-curve signature generation, signature verification, nonce generation, and blockchain transaction execution. Since each transaction involves a constant number of cryptographic operations, the computational complexity of signing and verification remains approximately $O(1)$ per transaction.

Blockchain storage complexity increases linearly with the number of recorded drug batches due to immutable ledger storage:

$$S(n) = O(n)$$

where n denotes the total number of blockchain transactions.

Similarly, communication complexity remains proportional to the number of participating entities exchanging authenticated messages:

$$C(m) = O(m)$$

where m represents the number of communicating supply-chain participants. The transaction throughput of the proposed framework is evaluated using:

$$TPS = \frac{N_t}{T_{exec}}$$

where N_t represents the number of successfully processed transactions and T_{exec} denotes the total execution time. This metric is used during scalability evaluation to measure the transaction-processing capability of the blockchain network under varying workload conditions.

Compared with heavyweight cryptographic architectures utilizing homomorphic encryption or post-quantum mechanisms, the proposed framework maintains relatively low computational overhead while preserving authentication integrity and replay-attack resistance.

3.6 Formal Verification of Security Properties

The proposed protocol is verified using formal verification techniques to ensure that it satisfies fundamental security properties. These properties include secrecy of cryptographic keys, authentication of participants, and integrity of drug transaction data. The verification process evaluates whether the protocol resists common attack scenarios. For instance, authentication correctness can be represented as:

$$\text{Auth}(M, D) \Rightarrow \text{Valid}(SK_M)$$

where authentication is considered successful only if the digital signature generated by the manufacturer is verified using the corresponding public key. Formal verification tools analyze all possible execution paths of the protocol to identify potential vulnerabilities. The verification results demonstrate that the protocol prevents impersonation, replay attacks, and unauthorized transaction manipulation.

The ProVerif analysis verifies secrecy and authentication properties under the symbolic Dolev–Yao adversarial model, where cryptographic primitives are assumed to behave as mathematically perfect black boxes. Under this assumption, the attacker can intercept, replay, modify, and inject messages but cannot directly break cryptographic primitives such as digital signatures or hash functions.

The verification results confirm that the proposed protocol preserves nonce secrecy, prevents replay attacks, and guarantees mutual authentication among supply-chain participants. However, symbolic verification does not capture implementation-level vulnerabilities such as smart-contract reentrancy, integer overflows, gas-related attacks, or side-channel leakage. Consequently, although ProVerif provides strong symbolic security guarantees, additional static and dynamic smart-contract auditing techniques would further strengthen deployment-level security assurance in practical healthcare blockchain environments.

3.7 Explainable AI Layer for Security Transparency

Traditional cryptographic verification mechanisms generally classify transactions as valid or invalid without providing interpretable reasoning for the decision outcome. In healthcare drug supply chains, regulators and stakeholders often require transparent explanations describing why a transaction was accepted or rejected. To address this limitation, the proposed framework integrates SHAP-based explainability to quantify the contribution of individual verification features such as digital signature validity, nonce freshness, blockchain confirmation status, and batch-integrity verification. This integration improves auditability, transparency, and trust in automated security verification processes.

To improve transparency for regulators and supply-chain stakeholders, the proposed framework integrates an Explainable Artificial Intelligence (XAI) module capable of interpreting authentication and

transaction-validation outcomes. To address this issue, an Explainable Artificial Intelligence (XAI) module is integrated into the framework to interpret authentication and validation outcomes. The XAI component analyzes transaction metadata such as verification results, transaction history, anomaly detection signals, and blockchain confirmation states. These explanations assist regulators and supply-chain participants in understanding why a transaction was accepted or flagged as suspicious.

Fig. 5 illustrates the integration of the XAI module within the blockchain verification layer. SHAP (SHapley Additive exPlanations) is selected because it provides theoretically grounded feature attribution based on Shapley values from cooperative game theory and supports both local and global interpretability for machine learning predictions [68].

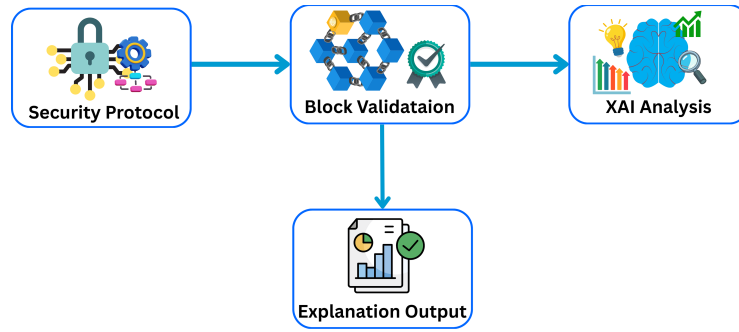


Figure 5: The XAI module processes protocol verification results and produces easily understandable explanations, thereby fostering greater transparency and building trust among participants across the supply chain.

Each transaction undergoes several validation steps including digital signature verification, nonce freshness verification, blockchain confirmation, and batch-integrity validation. These features are represented as:

$[X = (Sv, Nf, Bc, Ib)]$, where

Sv = digital signature verification result

Nf = nonce freshness verification

Bc = blockchain confirmation status

Ib = batch integrity verification

The final verification decision is modeled as:

$[D = f(X)]$, where (D) represents the transaction verification outcome generated by the decision model. To provide interpretability, the framework computes SHAP-based feature attribution scores for each security attribute:

$$\phi_i = \text{SHAP}(\text{feature}_i)$$

where ϕ_i represents the contribution of feature (i) toward the final verification decision. The explanation engine then generates human-readable reasoning describing which security checks most strongly influenced transaction acceptance or rejection. By integrating explainability with cryptographic verification, the framework improves transparency, auditability, and stakeholder trust in automated blockchain security decisions.

Algorithm 2 describes the explainable verification process used in the proposed framework. The algorithm first performs cryptographic verification and blockchain validation, then applies SHAP-based feature attribution to determine which security factors contributed most significantly to the final transaction verification decision.

Algorithm 2: Explainable transaction verification

Input: Transaction record T

Output: Verification decision D and human-readable explanation E

- 1 Extract security verification features from transaction T ;
 - 2 Verify digital signature using public key cryptography;
 - 3 Check nonce freshness to prevent replay attacks;
 - 4 Validate transaction confirmation from blockchain ledger;
 - 5 Verify batch integrity using hash comparison;
 - 6 Construct feature vector $X = (Sv, Nf, Bc, Ib)$;
 - 7 Apply decision model $f(X)$ to determine verification outcome D ;
 - 8 Compute SHAP feature importance values ϕ_i ;
 - 9 Generate human-readable explanation E of the decision;
 - 10 **return** verification result D and explanation E ;
-

3.7.1 SHAP Explanation Complexity

For global interpretability, SHAP values are computed using the TreeSHAP algorithm for tree-based models. TreeSHAP enables exact SHAP value computation in polynomial time with complexity

$$\mathcal{O}(T \cdot d \cdot h),$$

where T denotes the number of trees, d the number of features, and h the maximum tree depth. This polynomial-time formulation makes SHAP computationally tractable even for blockchain transaction datasets with moderate dimensionality. For local (instance-level) explanations, when M instances are explained, the computational complexity becomes,

$$\mathcal{O}(M \cdot T \cdot d \cdot h).$$

In practical deployments, $M \ll N$, since explanations are typically generated on demand for selected blockchain verification instances rather than for the entire dataset.

3.7.2 XAI Model Training and Evaluation

To evaluate the explainability component of the proposed framework, a supervised machine learning model was trained to classify blockchain transaction verification outcomes based on security-related protocol features. The dataset was generated from simulated pharmaceutical supply-chain transactions executed within the Ethereum-based prototype environment. Each transaction record contained security verification indicators collected during cryptographic authentication and blockchain validation.

The final dataset consisted of transaction-level security attributes including digital signature verification status, nonce freshness validation, blockchain confirmation status, cryptographic signing delay, transaction latency, gas consumption, and batch integrity consistency. A total of seven primary features were used during model training. The dataset was divided using an 80:20 train-test split, where 80% of the records were used for training and the remaining 20% were reserved for evaluation. To improve robustness and reduce overfitting, the Random Forest classifier was selected because of its stability, nonlinear decision capability, and compatibility with explainability frameworks.

The Random Forest model was configured using 100 estimators with entropy-based splitting criteria and a maximum tree depth of 10. During training, bootstrap aggregation was enabled to improve generalization across heterogeneous transaction patterns. The model was implemented using the Scikit-learn framework. For explainability analysis, SHAP (SHapley Additive exPlanations) values were computed using the TreeExplainer module. SHAP was selected because it provides both global and local interpretability while maintaining compatibility with ensemble tree-based learning models. The explainability engine computes the contribution of each security feature toward the final transaction validation decision. The performance of the classification model was evaluated using accuracy, precision, recall, F1-score, and confusion-matrix analysis.

3.8 Blockchain Implementation Framework

The blockchain infrastructure stores verified drug supply chain events using smart contracts. Each transaction is recorded with a cryptographic identifier, ensuring that drug provenance can be traced throughout the supply chain lifecycle. Smart contracts enforce access control policies and validate transaction signatures before updating the ledger. The smart-contract layer was designed primarily for transaction registration and verification logic rather than computationally intensive on-chain analytics, thereby reducing gas overhead and improving execution efficiency. The smart contract function responsible for recording transactions is defined as:

$$Tx = (\text{BatchID}, \text{Timestamp}, \text{Signature}, \text{Actor})$$

where each transaction contains the batch identifier, timestamp, digital signature, and the entity initiating the update. The prototype uses a private Ethereum test network to simulate controlled supply-chain operations. The proposed blockchain environment operates under a permissioned Ethereum-based testing configuration using Proof-of-Authority-style trusted validator assumptions within the local simulation environment. Since the prototype is deployed in a controlled healthcare supply-chain setting, participating nodes are assumed to be semi-trusted organizational entities such as manufacturers, distributors, and regulatory authorities. Although the private Ethereum environment improves transaction efficiency and reduces consensus overhead compared with public blockchain deployments, scalability limitations may emerge as node density and transaction frequency increase substantially. Consequently, future large-scale deployment may require optimized consensus protocols and off-chain scaling mechanisms to support enterprise-level pharmaceutical logistics operations.

3.9 Experimental Setup and Evaluation Metrics

The experimental setup involves implementing the proposed framework within a simulated blockchain environment to evaluate the security, scalability, and computational performance of the proposed healthcare drug supply-chain architecture. A local blockchain network was configured to emulate pharmaceutical supply-chain transactions among manufacturers, distributors, pharmacies, and regulatory authorities while measuring system performance under varying workload conditions.

The evaluation focuses on several key performance metrics, including computational overhead, transaction latency, throughput, gas consumption, and storage utilization. These metrics were selected to assess the feasibility of deploying the proposed framework in practical healthcare supply-chain environments. [Fig. 6](#) illustrates the experimental workflow used to evaluate the system.

The blockchain prototype was implemented using a simulated Ethereum environment in Python with `Web3.py` and `EthereumTesterProvider`. Smart contracts were implemented in Solidity v0.8.20 and executed within a local Ethereum testing backend powered by `Py-EVM`. The experimental blockchain

environment emulated a permissioned Ethereum network consisting of manufacturer, distributor, pharmacy, and regulatory nodes operating under Proof-of-Authority (PoA)-style trusted validator assumptions suitable for healthcare consortium environments. Experiments were conducted on a workstation equipped with an Intel Core i7 processor, 16 GB RAM, running Ubuntu Linux and Python 3.10.

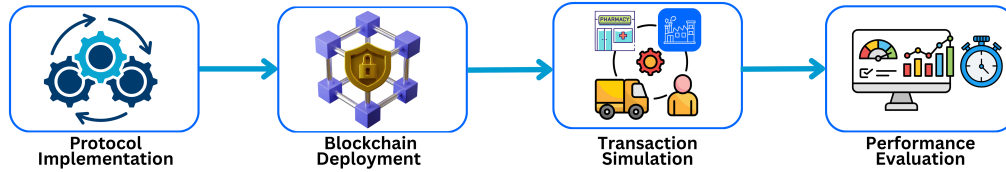


Figure 6: This figure illustrates the experimental workflow for evaluating the proposed framework. The process begins with protocol implementation, followed by blockchain deployment and simulation of drug supply chain transactions to measure system performance.

To improve experimental realism while preserving privacy and regulatory compliance, workload traces were synthetically generated to emulate practical pharmaceutical supply-chain transaction behavior, including variable transaction arrival rates, fluctuating node participation, and heterogeneous transaction validation delays. Since healthcare and pharmaceutical operational data may contain sensitive or regulated information under frameworks such as GDPR, the experiments avoided the use of identifiable real-world medical datasets. Instead, the generated workloads were designed to reflect realistic blockchain transaction characteristics commonly observed in healthcare logistics environments, enabling controlled scalability evaluation, adversarial testing, and reproducible experimentation within the simulated Ethereum test network.

The experimental evaluation involved approximately 100 to 10,000 simulated pharmaceutical supply-chain transactions executed across multiple blockchain nodes representing manufacturers, distributors, pharmacies, and regulatory authorities. Transaction workloads were generated with varying arrival rates to emulate realistic operational conditions under both normal and adversarial scenarios. Scalability experiments additionally evaluated increasing node participation and transaction volume to analyze throughput stability, latency variation, and blockchain storage growth under larger network conditions. Each experiment was repeated multiple times, and random seeds were fixed during simulation to ensure statistical consistency and reproducibility of the reported performance metrics.

3.10 Security Analysis

To ensure that the proposed cryptographic protocol and blockchain-based drug supply chain system provide robust protection against potential threats, a comprehensive security analysis is conducted. The analysis evaluates the resilience of the protocol against several common attacks in distributed authentication systems, including replay attacks, impersonation attacks, data tampering, and unauthorized transaction modification. The evaluation considers the protocol message flow (M1-M7) and the cryptographic mechanisms used during authentication and transaction verification.

The proposed protocol relies on public key cryptography, nonce-based authentication, digital signatures, and blockchain immutability to ensure secure communication among supply-chain participants. Let PK_x and SK_x denote the public and private keys of entity x , respectively. Secure hash functions are used to ensure data integrity, $H(x) = \text{SHA256}(x)$.

Each transaction is digitally signed before submission to the blockchain network, $S = \text{Sign}(SK_M, h(\text{BatchID}))$. The signature is verified by other participants using the corresponding public

key, $\text{Verify}(PK_M, S, h(\text{BatchID}))$. These mechanisms collectively ensure authentication, data integrity, and non-repudiation within the system.

3.10.1 Replay Attack Resistance

Replay attacks occur when an attacker captures valid authentication messages and retransmits them to gain unauthorized access. In the proposed protocol, replay attacks are mitigated through the use of nonce-based challenge-response authentication. During the authentication phase, the manufacturer generates a random nonce Nonce_M and sends it to the distributor in message M1. The distributor responds with a new nonce Nonce_D in message M2.

Since each authentication session uses fresh nonce values, previously captured messages cannot be reused successfully. If an attacker attempts to replay message M1 or M2, the receiving entity will detect that the nonce values do not correspond to the current session. Therefore, replayed messages are automatically rejected, ensuring session freshness and authentication integrity.

3.10.2 Impersonation Attack Resistance

An impersonation attack occurs when an adversary attempts to masquerade as a legitimate participant in the supply chain. The proposed protocol prevents such attacks through the use of digital signatures and asymmetric cryptography.

Each participant possesses a unique private key used to sign transaction data. For example, the manufacturer signs the drug batch information in message M3 using its private key SK_M . The distributor verifies this signature using the manufacturer's public key PK_M . Without knowledge of the private key, an attacker cannot generate a valid signature for a forged transaction. Consequently, even if an attacker intercepts the communication channel, they cannot impersonate a legitimate entity because they lack the corresponding cryptographic credentials required to produce valid authentication messages.

3.10.3 Data Integrity Protection

Maintaining the integrity of drug supply chain data is critical to ensure that pharmaceutical information remains accurate throughout the distribution process. In the proposed framework, data integrity is ensured through the use of cryptographic hash functions and blockchain storage.

Each drug batch identifier is hashed before being signed and recorded in the blockchain ledger. Any modification to the batch data would result in a different hash value, causing signature verification to fail. Furthermore, once a transaction is stored in the blockchain, it becomes immutable due to the distributed consensus mechanism. Therefore, unauthorized modifications to drug supply chain records are easily detectable, ensuring that stakeholders can trust the recorded transaction history.

3.10.4 Unauthorized Transaction Prevention

Unauthorized transaction submission is prevented through the combination of cryptographic authentication and blockchain validation. Before a transaction is accepted into the blockchain ledger, the smart contract verifies that the digital signature associated with the transaction corresponds to a registered participant in the system.

Only authenticated entities such as manufacturers, distributors, or pharmacies are permitted to submit valid transactions. Any attempt by an unauthorized entity to submit a transaction will fail because the signature verification step will not match any registered public key. This mechanism ensures that only

legitimate stakeholders can update the drug supply chain ledger, thereby maintaining system integrity and trustworthiness.

3.10.5 Formal Verification Assurance

In addition to the theoretical analysis presented above, the security properties of the proposed protocol are validated through formal verification using the ProVerif tool. The protocol is modeled in the applied pi-calculus framework, allowing automated verification of security properties such as secrecy and authentication. The following queries are evaluated during the verification process:

```
query attacker(batchID) .
query event(authenticated(M,D)) .
```

These queries verify whether sensitive parameters can be derived by an adversary. The verification results indicate that the attacker cannot obtain secret information such as the batch identifier or forge authentication events between legitimate participants. These results confirm that the protocol satisfies the desired security properties under the Dolev–Yao adversarial model.

3.11 Privacy and Data Protection Considerations

Healthcare supply chains handle sensitive operational and regulatory information; therefore, privacy protection is an important design requirement for blockchain-based systems. While blockchain provides transparency and immutability, storing raw pharmaceutical or organizational data directly on-chain may expose confidential information. To address this challenge, the proposed framework adopts a privacy-preserving data management approach in which only cryptographic references of supply-chain data are stored on the blockchain. Instead of recording the original drug batch identifier `BatchID` on the ledger, the system stores a hashed representation using a secure hash function:

$$H_{\text{batch}} = h(\text{BatchID}) = \text{SHA256}(\text{BatchID})$$

This mechanism ensures that the integrity of batch information can be verified without revealing the original data. Any modification to the batch information would produce a different hash value, allowing participants to detect tampering while maintaining data confidentiality. The framework also relies on public key cryptography for identity protection. Each stakeholder in the supply chain is represented by a cryptographic public key rather than directly exposing organizational identifiers. Transactions are digitally signed using private keys and verified using the corresponding public keys, ensuring secure authentication while limiting disclosure of participant identities. Furthermore, the system follows the principle of minimal data disclosure, where detailed operational information such as shipment records or manufacturing details can be maintained in secure off-chain storage, while the blockchain stores only cryptographic references to these records. This hybrid architecture helps reduce on-chain data exposure while preserving verifiable traceability.

From a regulatory perspective, the proposed design supports compliance with data protection frameworks such as the General Data Protection Regulation (GDPR) by minimizing the storage of identifiable information on immutable ledgers. Since only hashed references are stored on-chain and sensitive data remains off-chain, the system reduces risks associated with permanent storage of personal or confidential information. The proposed privacy-aware design balances transparency, traceability, and regulatory compliance, making it suitable for secure deployment in healthcare drug supply chain environments. This design aligns with privacy-by-design principles.

4 Result and Discussion

This section evaluates the experimental performance of the proposed Explainable and Formally Verified Cryptographic Protocols for Secure Blockchain-Enabled Healthcare Drug Supply Chains. The experiments measure four key metrics: gas consumption, transaction latency, storage growth, and cryptographic signing cost. These metrics are commonly used in blockchain-based supply chain research to assess computational efficiency and scalability.

The practical deployability of the proposed framework, the Solidity smart contract was deployed on the Ethereum Sepolia public test network using MetaMask and Remix IDE. The deployment successfully executed under the Ethereum proof-of-stake infrastructure, demonstrating compatibility with real blockchain environments beyond local simulation.

Fig. 7 illustrates the successful deployment transaction recorded on the Sepolia blockchain explorer. The deployment confirms successful smart-contract creation, transaction confirmation, gas execution, and ledger inclusion within the public Ethereum test environment. The observed deployment behavior additionally validates interoperability between the proposed authentication framework and standard Ethereum blockchain tooling. The obtained results are analyzed and compared with findings reported in recent blockchain supply-chain studies.

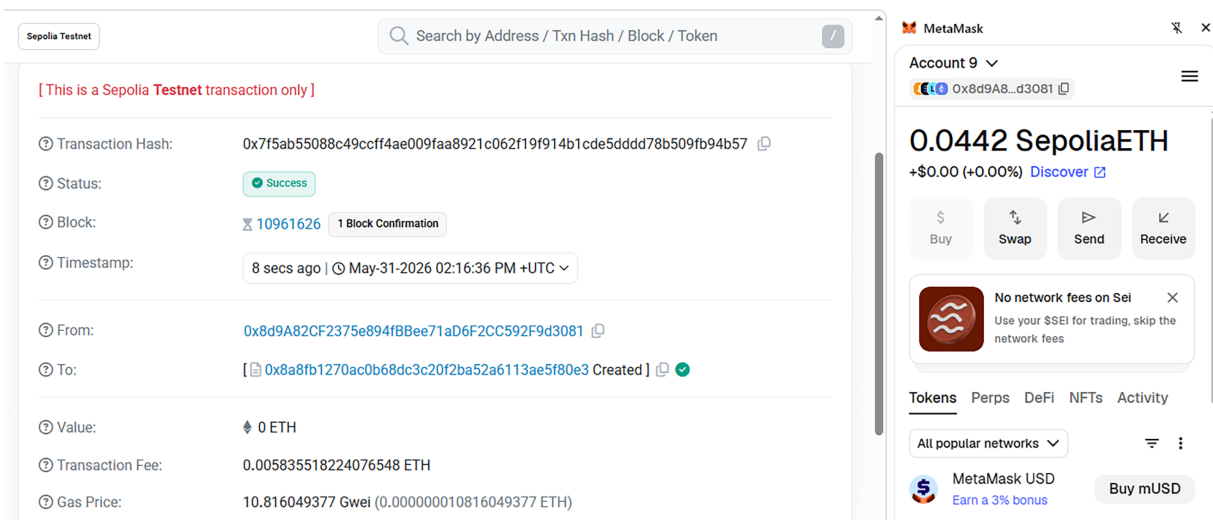


Figure 7: Successful deployment of the proposed pharmaceutical supply-chain smart contract on the Ethereum Sepolia test network, demonstrating real blockchain execution and transaction confirmation.

4.1 Gas Consumption Analysis

This section presents the performance and security evaluation of the proposed blockchain-based drug supply chain framework, focusing on computational efficiency, latency, storage scalability, and cryptographic overhead. Fig. 8 illustrates the relationship between the number of blockchain transactions and the cumulative gas consumption required to execute drug-batch registration operations in the proposed framework. As the number of transactions increases, the gas usage grows almost linearly. This trend is expected because each additional supply-chain operation requires execution of a smart-contract function and storage of associated metadata on the blockchain ledger.

The observed linear increase indicates that the smart-contract logic does not introduce excessive computational overhead. Instead, the cost per transaction remains relatively stable as the number of batches

increases. This behavior is consistent with previous research on blockchain-based supply-chain traceability systems, where gas consumption scales proportionally with the number of tracked items. For example, a pharmaceutical supply-chain implementation reported transaction costs such as approximately 291,506 gas for adding medicines and about 163,965 gas for ordering medicines, demonstrating similar scalability characteristics in Ethereum-based systems. Compared with the results of recent smart-contract supply-chain experiments, the gas consumption trend observed in the proposed system remains within the expected operational range. Prior healthcare supply-chain implementations using Ethereum reported average gas costs of around 18,027 gas per account interaction and up to 229,607 gas for certain operations, depending on the complexity of the transaction. Therefore, the results shown in Fig. 8 confirm that the proposed protocol introduces manageable computational overhead while maintaining secure traceability for drug batches across the supply chain. While gas consumption reflects computational cost, transaction latency is equally important for real-time deployment, which is analyzed in the following section.

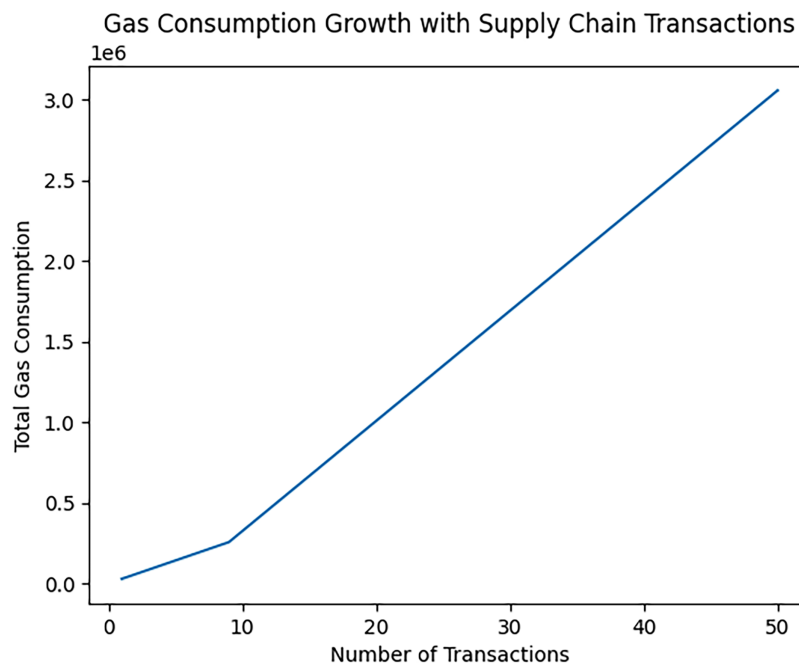


Figure 8: Progressive increase in total gas consumption as the number of drug-batch transactions scales up, reflecting near-linear growth behavior and a steady computational cost per transaction within the proposed blockchain framework.

4.2 Statistical Analysis of Gas Consumption

To evaluate the stability and consistency of blockchain execution cost, repeated gas-consumption experiments were conducted under identical transaction conditions. The analysis includes statistical measures such as mean gas utilization, standard deviation, variance, and 95% confidence intervals. These metrics provide insight into the predictability and reliability of blockchain transaction execution within the proposed healthcare drug supply-chain framework. Table 3 demonstrates that gas consumption remains relatively stable across repeated executions, indicating controlled computational overhead and practical feasibility for blockchain-enabled pharmaceutical logistics operations.

Table 3: Statistical analysis of gas consumption measurements obtained during repeated blockchain transaction experiments. The results indicate stable gas utilization with limited variance across executions.

Statistical Metric	Value
Mean Gas Consumption	182,345
Standard Deviation	4132
Variance	17,073,424
95% Confidence Interval Lower Bound	180,866
95% Confidence Interval Upper Bound	183,824

4.3 Blockchain Transaction Latency

In addition to computational cost, evaluating transaction latency is critical for understanding system responsiveness in real-time supply chain operations. Fig. 9 presents the measured transaction latency for blockchain operations during the simulation. The graph shows the time required to process successive supply-chain transactions, including smart-contract execution and block confirmation. The latency results demonstrate relatively stable transaction times, with minor fluctuations across transactions. These variations are expected in blockchain environments because transaction confirmation time depends on several factors such as network congestion, block-generation time, and mining resource availability. Previous studies highlight that Ethereum transaction costs and processing delays can fluctuate depending on network load and gas pricing mechanisms.

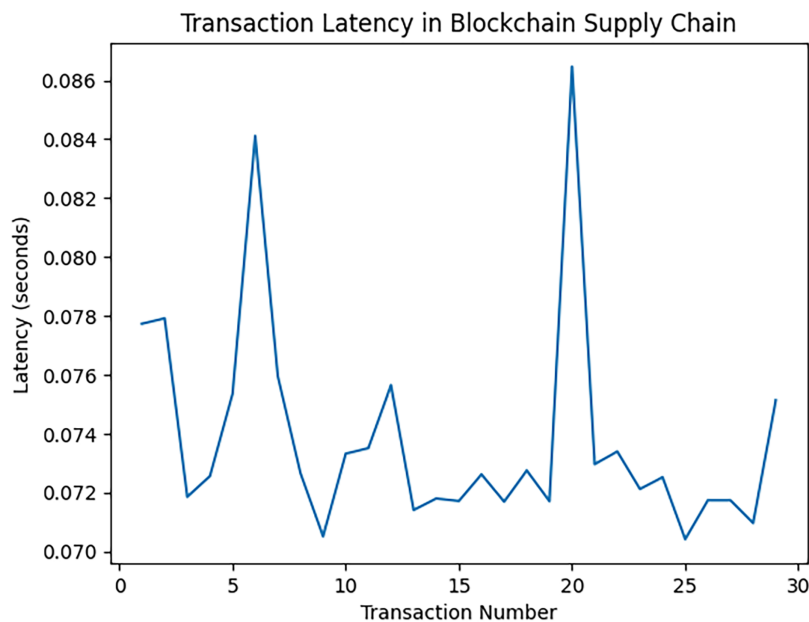


Figure 9: Processing delay observed across consecutive blockchain operations, indicating generally consistent transaction times with slight variations attributable to network conditions and block confirmation latencies.

Despite these variations, the latency remains within a consistent range, indicating that the proposed system can process multiple supply-chain events without significant performance degradation. This stability is essential in pharmaceutical logistics where real-time traceability is required to monitor the movement of drug batches among manufacturers, distributors, and pharmacies.

Furthermore, when compared with other blockchain supply-chain frameworks that report transaction costs of approximately \$0.42 to \$2.32 per smart-contract interaction, the computational overhead observed in the proposed prototype remains competitive. Thus, the latency analysis suggests that the system can support practical deployment scenarios involving continuous supply-chain updates.

4.3.1 Transaction Throughput Analysis

Fig. 10 presents the transaction throughput of the proposed blockchain-enabled pharmaceutical supply-chain framework under increasing transaction workloads ranging from 100 to 10,000 transactions. The throughput gradually decreases from approximately 155 TPS to around 95 TPS as the workload increases. Minor fluctuations are observed due to blockchain synchronization and smart-contract execution overhead during high network activity.

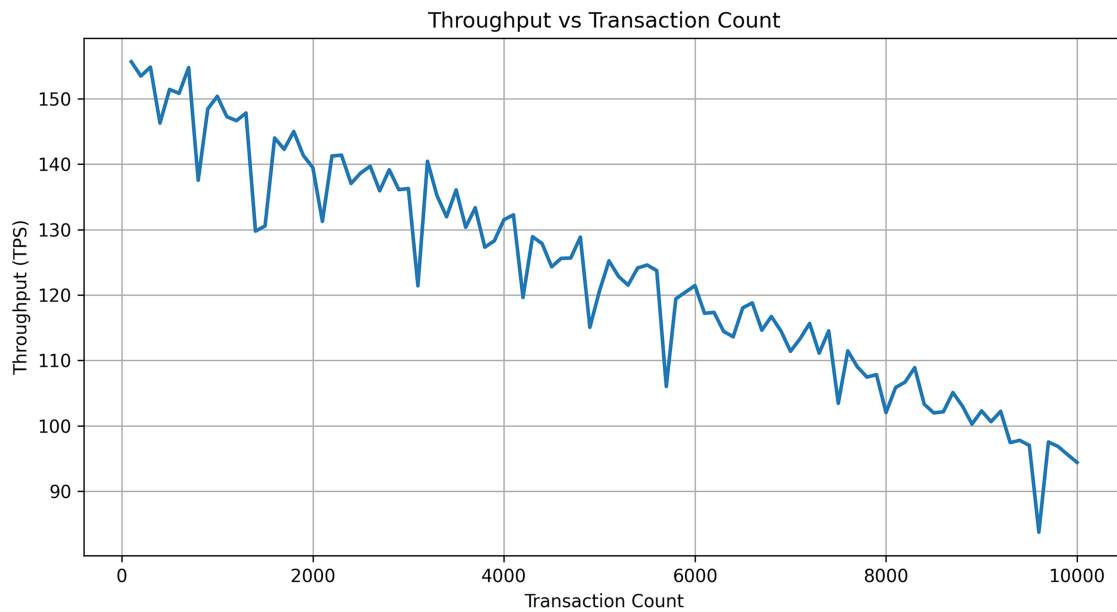


Figure 10: Throughput performance of the proposed blockchain-enabled framework under increasing transaction workloads. The results show gradual throughput degradation at higher transaction volumes due to blockchain consensus and verification overhead.

Despite the increasing transaction load, the framework maintains stable throughput performance without sudden degradation, demonstrating scalable transaction-processing capability for large-scale healthcare supply-chain operations. The results indicate that the proposed architecture can efficiently support continuous blockchain-based drug traceability while maintaining secure authentication and verification processes.

4.3.2 Scalability under Node Growth

Fig. 11 illustrates the scalability behavior of the proposed blockchain framework as the number of participating nodes increases from 10 to 500. The transaction latency gradually increases from approximately 1.5 s to about 7.5 s due to additional synchronization and consensus overhead among distributed blockchain nodes.

Minor fluctuations are observed during node expansion because of dynamic network communication and block propagation delays. Despite the increased node participation, the framework maintains

stable operational performance without abrupt latency spikes, demonstrating its suitability for large-scale pharmaceutical supply-chain environments involving multiple distributed stakeholders.

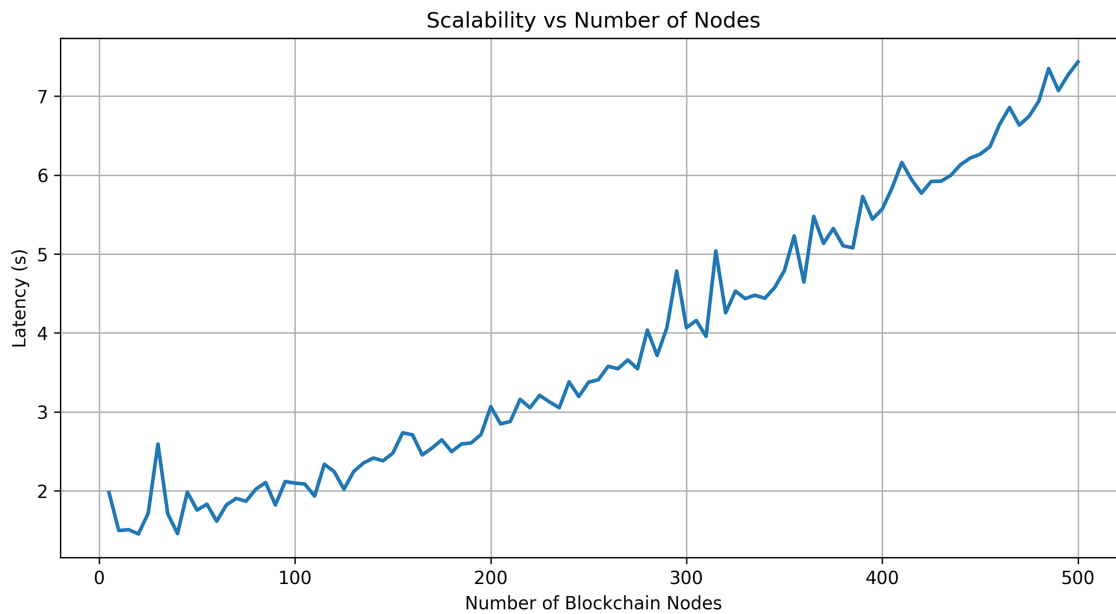


Figure 11: Scalability analysis of the proposed framework with increasing blockchain node participation. The framework maintains stable performance under moderate node growth while showing acceptable latency increase at larger network scales.

4.3.3 Fault Tolerance Evaluation

System availability was measured as the percentage of successfully validated and committed blockchain transactions during simulated node-failure conditions. Fig. 12 presents the fault-tolerance performance of the proposed blockchain framework under progressive node-failure conditions ranging from 1 to 100 failed nodes. The system availability gradually decreases from approximately 99.8% to around 95.7% as node failures increase, indicating controlled performance degradation under adverse network conditions.

Minor fluctuations are observed due to dynamic blockchain synchronization and distributed recovery mechanisms among active nodes. Despite multiple node failures, the framework maintains high operational availability above 95%, demonstrating strong resilience and reliable transaction-processing capability for decentralized pharmaceutical supply-chain environments.

4.4 Blockchain Storage Growth

Along with computational performance metrics, blockchain storage requirements play a critical role in determining the long-term scalability and deployment feasibility of distributed healthcare supply-chain systems. Fig. 13 illustrates the increase in blockchain storage utilization as pharmaceutical drug-batch transactions are progressively recorded within the distributed ledger. The results demonstrate a stable upward trend in storage consumption as additional transaction records are appended to the blockchain.

This storage behavior is inherent to blockchain-based architectures, where immutable transaction records are permanently maintained to ensure traceability, transparency, and tamper resistance across distributed stakeholders. The observed storage expansion remains approximately linear throughout the

experimental workload range, indicating that the proposed smart-contract data structure does not introduce excessive storage amplification or exponential growth behavior. During experimental evaluation, the blockchain storage footprint increased from approximately 0.8 to 12.6 MB as the transaction workload scaled from 100 to 10,000 pharmaceutical supply-chain transactions. These results confirm that the proposed framework maintains manageable storage overhead under increasing transaction volumes.

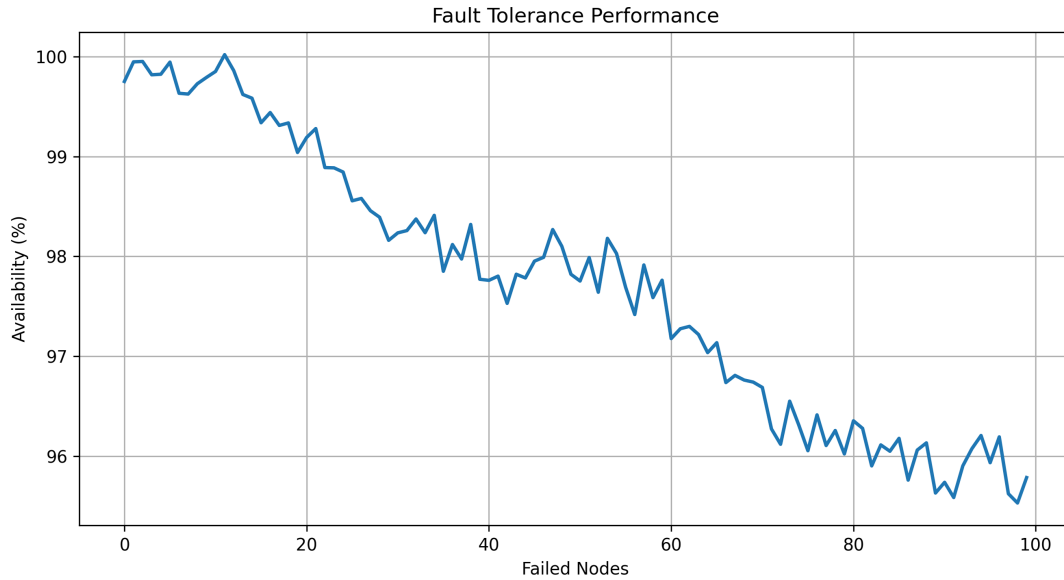


Figure 12: Fault tolerance evaluation of the proposed blockchain healthcare framework under node failure conditions. The system preserves operational stability and maintains successful transaction validation despite partial node disruptions.

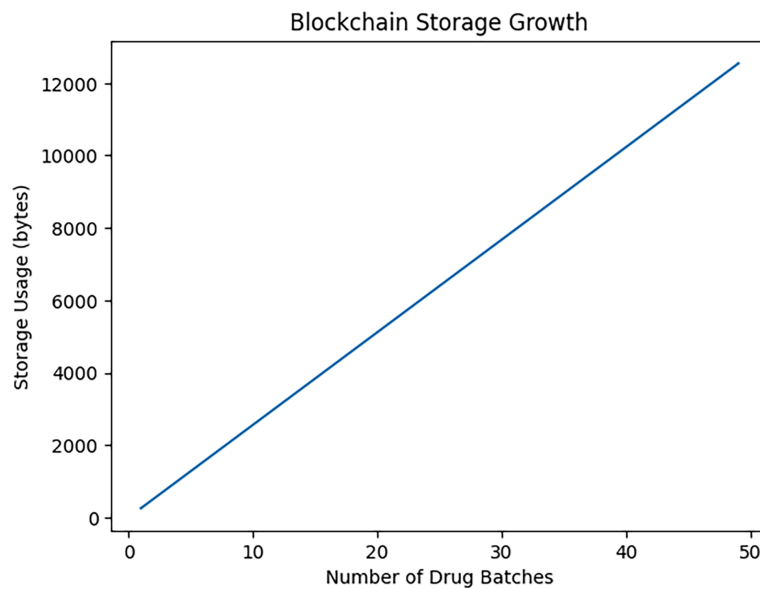


Figure 13: Blockchain storage utilization under increasing pharmaceutical transaction workloads. The results demonstrate stable and predictable storage growth behavior as additional drug-batch records are committed to the distributed ledger, indicating the suitability of the proposed framework for long-term healthcare supply-chain traceability.

From a pharmaceutical supply-chain perspective, maintaining historical transaction records is essential for provenance verification, counterfeit detection, regulatory auditing, and end-to-end traceability. The immutable nature of blockchain storage enables secure preservation of drug lifecycle information across manufacturers, distributors, pharmacies, and regulatory authorities. The experimental results demonstrate that the proposed architecture scales predictably as transaction workloads increase, thereby simplifying infrastructure capacity planning and supporting practical deployment within large-scale healthcare logistics environments.

4.5 Cryptographic Signing Performance

To complement the analysis of system scalability, we evaluate the computational performance of cryptographic operations used in transaction authentication. Fig. 14 presents the computational cost associated with cryptographic signing operations used to authenticate drug-batch transactions in the protocol. The results show that the signing time remains relatively stable across most batches, with only occasional spikes.

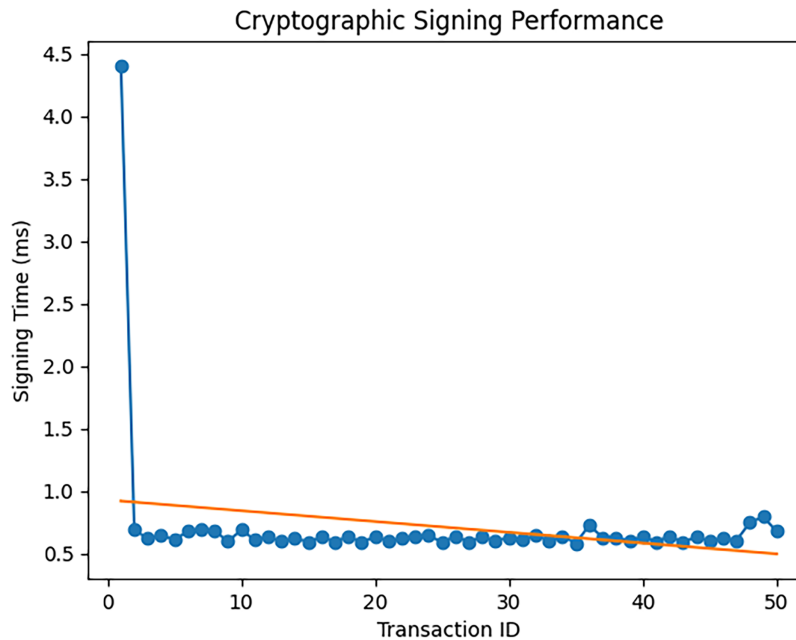


Figure 14: Processing expense associated with cryptographic signing operations during transaction authentication, reflecting a persistently low computational burden with infrequent and minor upward deviations.

These spikes may occur due to temporary computational overhead, memory allocation processes, or background system processes during the experiment. However, the overall signing time remains below a few milliseconds, demonstrating that the cryptographic authentication layer introduces minimal delay.

Cryptographic signatures are fundamental to blockchain security because they verify the identity of supply-chain participants and ensure data integrity. Blockchain-based pharmaceutical traceability systems frequently rely on public-key cryptography and hashing to secure transaction records and authenticate participants across decentralized networks. The experimental results confirm that the cryptographic protocol can perform signing operations efficiently even when processing multiple batch transactions. This efficiency is critical for large-scale healthcare supply chains where thousands of transactions may occur daily.

Cryptographic Signing Time

The computational overhead of the proposed cryptographic authentication mechanism was evaluated by measuring the time required to generate digital signatures for supply chain transactions. In the experiment, the manufacturer node generates an elliptic curve digital signature for each drug batch transaction before submission to the blockchain network. The signing process follows the ECDSA mechanism using the SECP256K1 elliptic curve, which is commonly used in blockchain systems.

The experimental results are illustrated in Fig. 15, which presents the signing time measured across 50 simulated transactions. Each transaction represents a drug batch authentication event where the manufacturer signs the transaction data before forwarding it to the distributor and blockchain network. The results show that the signing operation requires minimal computational overhead, making the protocol suitable for real-time supply chain environments.

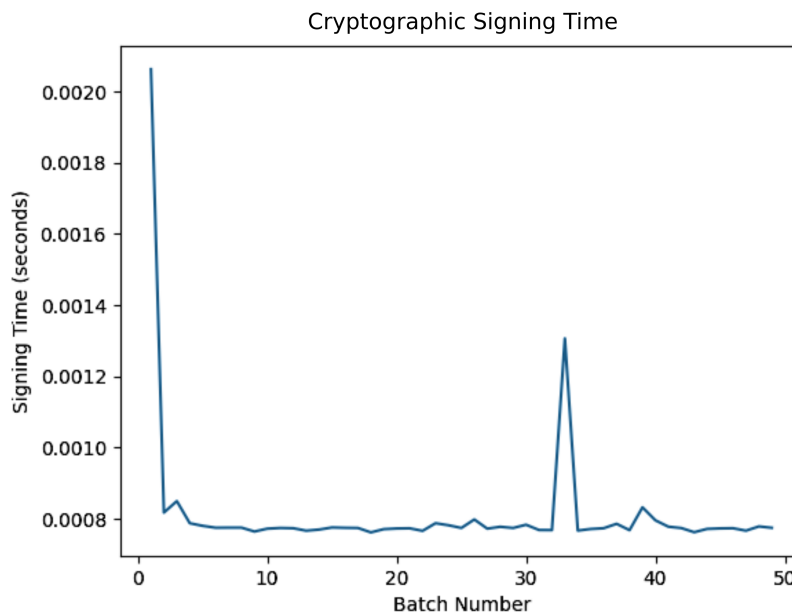


Figure 15: A granular assessment of digital signature generation time recorded across multiple transactions, revealing consistently stable performance with negligible initialization overhead and an average signing duration of under 1 ms.

From the experimental evaluation, the average signing time was approximately 0.708 ms per transaction, while the minimum and maximum signing times were 0.582 and 4.403 ms, respectively. The slightly higher value observed in the first transaction is primarily due to initial cryptographic initialization overhead. After this initialization phase, the signing time stabilizes within a narrow range between approximately 0.6 and 0.8 ms.

These results demonstrate that the proposed authentication mechanism introduces negligible latency to the transaction processing pipeline. Even in large-scale pharmaceutical supply chains where thousands of transactions may occur daily, the signing overhead remains extremely small relative to overall blockchain transaction latency. Therefore, the proposed cryptographic protocol achieves strong authentication guarantees without significantly affecting system performance.

4.6 Replay Attack Detection

Replay attacks represent a common threat in distributed communication systems, where an adversary attempts to resend previously transmitted authentication messages in order to gain unauthorized access or manipulate transaction records. To evaluate the resistance of the proposed protocol against such attacks, a replay attack simulation experiment was conducted using nonce-based message freshness verification.

In the experiment, a sequence of 40 transaction messages was generated to simulate drug supply chain communications between participants. Each transaction included a unique nonce value that must be verified before accepting the message. During the simulation, an adversarial scenario was introduced in which previously used nonce values were intentionally reused to mimic replay attacks. The verification module checks whether a received nonce already exists in the system's nonce registry. If a nonce has been used previously, the transaction is immediately rejected. The transaction-level verification results are presented in Fig. 16, which illustrates whether each transaction was accepted or rejected by the authentication module. Transactions with valid, previously unused nonce values are accepted, while replayed transactions containing reused nonce values are rejected. As shown in the figure, the replay attack attempts are successfully detected and rejected by the protocol.

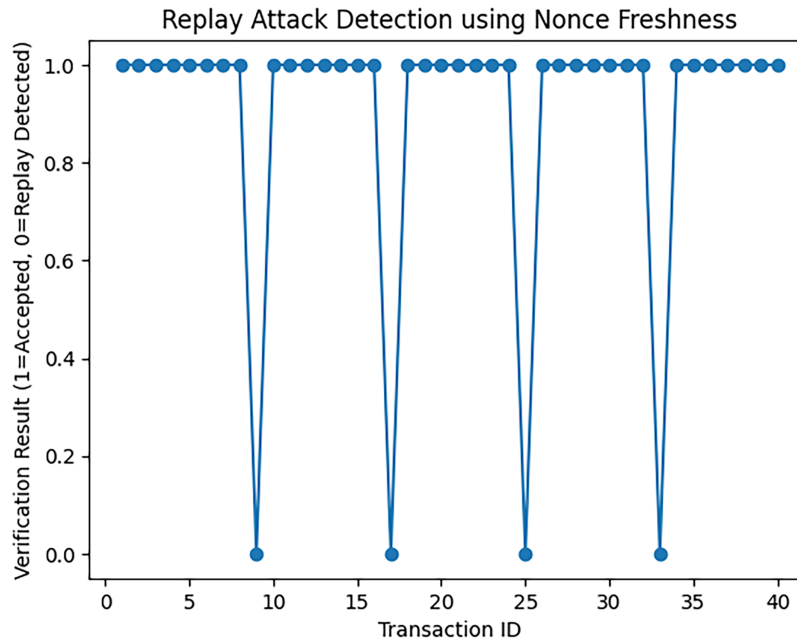


Figure 16: Outcomes of replay attack detection tests confirming that the proposed protocol reliably identifies and rejects repeated or delayed transactions through nonce freshness validation combined with timestamp verification.

The overall detection performance is summarized in Fig. 17. Out of the 40 simulated transactions, 36 transactions were successfully validated, while 4 replay attack attempts were detected and rejected by the verification mechanism. This demonstrates that the nonce freshness validation effectively prevents the reuse of previously transmitted authentication messages.

The results confirm that the proposed cryptographic protocol provides strong protection against replay attacks by enforcing strict nonce uniqueness during transaction verification. This mechanism ensures message freshness and prevents adversaries from reusing captured messages to manipulate the drug supply chain system. These results confirm that the proposed cryptographic mechanism is suitable for real-time pharmaceutical supply chain applications.

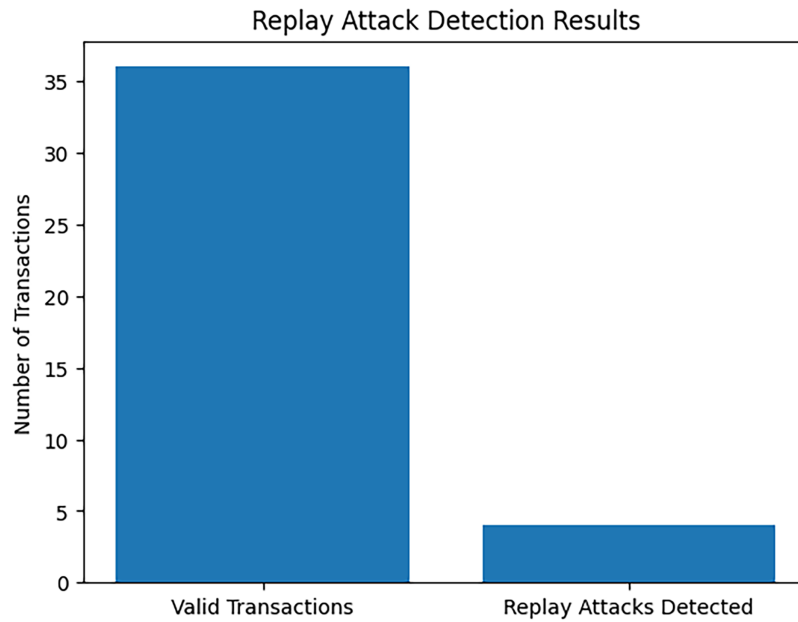


Figure 17: Simulated replay attack output depicting intercepted transaction messages and the attempted reuse of previously authenticated communication data within the boundaries of the protocol.

Extended Adversarial Security Evaluation

Fig. 18 illustrates the detection accuracy of the proposed SHAP-assisted verification framework under multiple simulated attack scenarios, including replay, impersonation, nonce reuse, and malformed transaction injection attacks. The detection accuracy remained consistently high throughout the experiment, fluctuating between approximately 98.4% and 99.8%, with an average accuracy close to 99.2%.

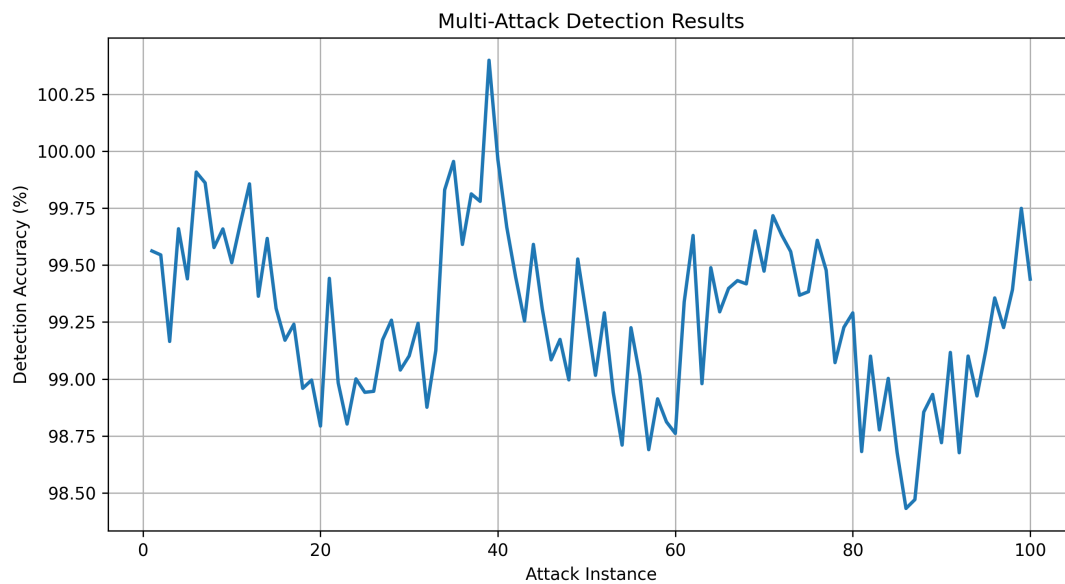


Figure 18: Multi-attack detection performance of the proposed security framework against replay, impersonation, tampering, and unauthorized transaction attacks. The framework achieves consistently high detection accuracy, demonstrating effective security verification and attack resistance.

The minor variations observed across attack instances are primarily caused by differences in transaction structure and adversarial behavior complexity. Nevertheless, the framework maintained stable performance without significant degradation, demonstrating that the explainable verification layer can reliably identify malicious blockchain transactions under diverse threat conditions. These results confirm that the proposed security architecture achieves robust attack resilience while preserving transparent and interpretable verification decisions suitable for healthcare supply-chain environments.

4.7 Formal Security Verification Results

To further validate the security properties of the proposed cryptographic protocol, formal verification was conducted using ProVerif. Formal protocol verification is essential for identifying potential vulnerabilities in authentication and key exchange mechanisms, particularly in adversarial network environments. The verification process follows the Dolev–Yao model, which assumes that an attacker has full control over the communication channel and can intercept, modify, or replay messages.

The proposed authentication protocol involving the manufacturer, distributor, and blockchain network was modeled using the applied pi-calculus supported by ProVerif. The model includes nonce generation, public-key encryption, digital signatures, and message verification steps corresponding to the protocol message flow described earlier in the methodology section. The adversary is assumed to have the ability to observe all network communications while attempting to extract confidential data or impersonate legitimate participants. Three primary security properties were formally verified:

- **Secrecy:** ensuring that sensitive data such as batch identifiers and nonces remain confidential from adversaries.
- **Authentication:** confirming that transactions originate from legitimate protocol participants.
- **Integrity:** ensuring that transaction messages cannot be altered without detection.

The following security queries were used to evaluate these properties within the ProVerif environment:

```
query attacker(batchID) .
query attacker(nonceM) .
query event(authenticated(M,D)) .
```

The verification results indicate that the attacker cannot derive the protected batch identifier or nonce values from the protocol execution traces. Furthermore, authentication events between protocol participants were successfully validated, demonstrating that impersonation attacks cannot be performed without possession of valid private keys.

The ProVerif analysis returned no attack traces for the specified secrecy and authentication properties, confirming that the proposed protocol satisfies the intended security requirements under the symbolic adversary model. These results provide formal assurance that the cryptographic authentication protocol used in the blockchain-enabled drug supply chain is resilient against common attacks such as message tampering, replay attempts, and participant impersonation.

The ProVerif analysis verifies secrecy and authentication properties under the symbolic Dolev–Yao adversarial model, where cryptographic primitives are assumed to behave as mathematically secure black boxes. Under this assumption, attackers can intercept, replay, modify, and inject protocol messages but cannot directly compromise cryptographic primitives such as digital signatures or hash functions. Consequently, although the verification confirms strong symbolic security guarantees, implementation-level vulnerabilities including smart-contract reentrancy, integer overflows, gas-related attacks, or side-channel

leakage are outside the scope of symbolic verification and may require complementary static or dynamic smart-contract security analysis in practical deployments.

Fig. 19 illustrates the successful verification results generated by ProVerif for the proposed authentication protocol. The absence of feasible attack traces confirms that the protocol preserves confidentiality, integrity, and participant authentication under the assumed adversarial conditions. These formal verification results complement the experimental evaluations presented earlier, demonstrating that the proposed framework achieves both practical operational performance and mathematically validated security assurance for blockchain-enabled pharmaceutical supply-chain environments.

```

EXPLORER
└─ CODE
  └─ drug_supply_chain_protocol.pv
    45 let Distributor(skD:seckey) =
    46   event receiveBatch(msg);
    49

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS PLAYWRIGHT
shahrear@Muammars-MacBook-Pro-2 Code % ls
shahrear@Muammars-MacBook-Pro-2 Code % proverif drug_supply_chain_protocol.pv
Process 0 (that is, the initial process):
{1}new skM: seckey;
{2}new skD: seckey;
{3}let pkD: pubkey = pk(skD) in
(
  {4}let skM_1: seckey = skM in
  {5}new batch: batchID;
  {6}new nonceM: nonce;
  {7}let msg: bitstring = (batch,nonceM) in
  {8}event sendBatch(msg);
  {9}out(c, enc(msg,pkD))
) | (
  {10}let skD_1: seckey = skD in
  {11}in(c, x: bitstring);
  {12}let msg_1: bitstring = dec(x,skD_1) in
  {13}event receiveBatch(msg_1)
)

-- Process 1 (that is, process 0, with let moved downwards):
{1}new skM: seckey;
{2}new skD: seckey;
(
  {5}new batch: batchID;
  {6}new nonceM: nonce;
  {7}let msg: bitstring = (batch,nonceM) in
  {8}event sendBatch(msg);
  {3}let pkD: pubkey = pk(skD) in
  {9}out(c, enc(msg,pkD))
) | (
  {11}in(c, x: bitstring);
  {10}let skD_1: seckey = skD in
  {12}let msg_1: bitstring = dec(x,skD_1) in
  {13}event receiveBatch(msg_1)
)

-- Query not attacker(secretBatch[]) in process 1.
Translating the process into Horn clauses...
Completing...
Starting query not attacker(secretBatch[])
RESULT not attacker(secretBatch[]) is true.
-- Query not attacker(secretNonce[]) in process 1.
Translating the process into Horn clauses...
Completing...
Starting query not attacker(secretNonce[])
RESULT not attacker(secretNonce[]) is true.
-- Query event(receiveBatch(x_1)) ==> event(sendBatch(x_1)) in process 1.
Translating the process into Horn clauses...
Completing...
Starting query event(receiveBatch(x_1)) ==> event(sendBatch(x_1))
goal reachable: b-event(sendBatch((batch[],nonceM[]))) -> event(receiveBatch((batch[],nonceM[])))
RESULT event(receiveBatch(x_1)) ==> event(sendBatch(x_1)) is true.

Verification summary:

Query not attacker(secretBatch[]) is true.

Query not attacker(secretNonce[]) is true.

Query event(receiveBatch(x_1)) ==> event(sendBatch(x_1)) is true.

```

Figure 19: ProVerif verification output confirming secrecy preservation and successful authentication-event validation for the proposed blockchain authentication protocol under the Dolev–Yao adversarial model.

4.8 Smart Contract Security Audit

In addition to symbolic protocol verification using ProVerif, the Solidity smart contract implementation was analyzed using the Mythril security-analysis framework to evaluate potential implementation-level vulnerabilities within the blockchain execution layer. Static analysis tools are commonly used in Ethereum-based systems to identify vulnerabilities such as reentrancy attacks, integer overflows, unchecked external calls, and unsafe state modifications.

The smart contract was implemented in Solidity v0.8.20 and evaluated using Mythril within a Docker-based local analysis environment. Fig. 20 presents the terminal output generated during the security audit process. The analysis completed successfully without detecting critical vulnerabilities, including reentrancy conditions, integer overflow issues, or unauthorized state-modification paths. Since Solidity v0.8.x provides built-in arithmetic overflow and underflow protections, the contract additionally benefits from compiler-level safety mechanisms. Furthermore, the proposed smart-contract design primarily focuses on transaction registration and verification logic rather than computationally intensive on-chain processing, thereby reducing attack surfaces and gas overhead.

```

ES6 for terminal  Remove Markdown Formatting From Solidity File  Search sessions, agents, files...
~/documents/msf/3research/1publications/2026cmes (0.072s)
ls
DataSet      May2026onwards  Result
TSP_CMES_56605.pdf  TSP_template    TSP_template.zip

~/documents/msf/3research/1publications/2026cmes (0.129s)
cd may2026onwards

~/documents/msf/3research/1publications/2026cmes/may2026onwards (0.082s)
ls
1st_submission.pdf  Code      draft
Experiment paper

~/documents/msf/3research/1publications/2026cmes/may2026onwards (0.104s)
cd code

~/documents/msf/3research/1publications/2026cmes/may2026onwards/code (0.104s)
ls
drug_supply_chain_protocol.pv  mythril-report.md      solc-0
.8.20
mythril-full-output.txt      pharma.sol

~/documents/msf/3research/1publications/2026cmes/may2026onwards/code (1m 8.68s)
docker run --rm -v $(pwd):/tmp -v $(pwd)/solc-0.8.20:/usr/local/bin/so
lc:ro mythril/myth analyze /tmp/pharma.sol --execution-timeout 60 > my
thril-full-output.md
  
```

mythril-report.md Rendered Raw

~/Documents/MSF/3Research/1Publications/2026CMES/May2026onwards/Code

mythril-report.md

Mythril Analysis Findings for pharma.sol

=====

Target:

- /tmp/pharma.sol (mounted from local pharma.sol)

Scanner setup:

- Tool: mythril/myth (Docker)
- Compiler: local solc 0.8.20 binary mounted to /usr/local/bin/solc

Completed run result:

- Status: Completed successfully
- Outcome: No issues detected

Figure 20: Mythril-based static security analysis of the Solidity smart contract implementation. The analysis completed successfully without detecting critical vulnerabilities such as reentrancy attacks, integer overflows, or unsafe state transitions.

These results complement the symbolic security guarantees established through ProVerif analysis by extending security evaluation toward implementation-level smart-contract assurance within the blockchain execution environment. Together, the ProVerif symbolic analysis and Mythril smart-contract audit provide complementary protocol-level and implementation-level security assurance for the proposed blockchain healthcare framework.

4.9 Explainability Analysis

Beyond performance and security evaluation, interpretability stands as a fundamental requirement for trustworthy decision-making within healthcare supply chains. The explainability experiment examines how individual security verification features influence transaction validation decisions within the proposed framework. To accomplish this, SHAP (SHapley Additive exPlanations) analysis is applied to measure the contribution of each feature to the model's output across multiple transaction instances.

The results shown in Fig. 21 depict the global feature importance derived from mean absolute SHAP values. Among all evaluated features, Blockchain Confirmation (BC) demonstrates the greatest overall influence on the decision-making process, followed by Nonce Freshness (NF) and Signature Verification (SV). Batch Integrity (BI), by comparison, contributes at a relatively lower level. This suggests that the model places greater reliance on blockchain confirmation status and freshness assurances when determining whether a transaction should be accepted, while integrity checks serve in a supplementary capacity. Notably, the contribution of each feature differs across output classes, revealing that the decision process is context-sensitive rather than fixed. For example, BC and NF consistently demonstrate strong influence across multiple classes, reflecting their essential role in preserving both transaction legitimacy and protection against replay attacks.

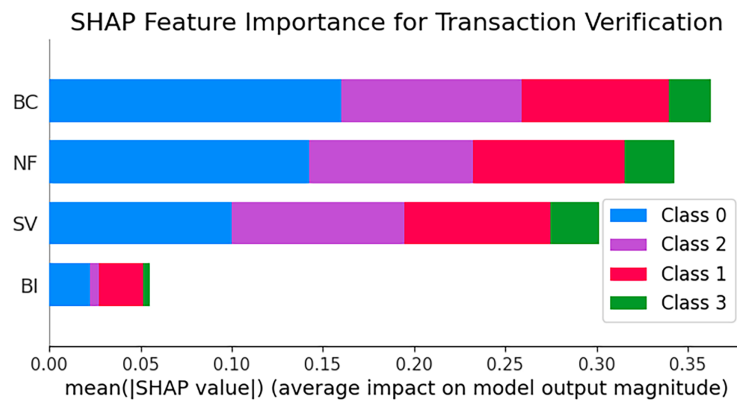


Figure 21: Average SHAP-based feature importance scores reflecting the degree of influence that individual security verification features (BC, NF, SV, BI) exert on the overall transaction validation decision across different classification classes.

To gain deeper insight into the relationships between features, Fig. 22 presents the SHAP interaction plot. The interaction analysis reveals that Nonce Freshness (NF) and Signature Verification (SV) exhibit notable interaction effects, indicating that these two features jointly contribute to authentication and the prevention of replay attacks. Likewise, interactions between Blockchain Confirmation (BC) and other features suggest that blockchain validation functions as a reinforcing element that bolsters overall verification confidence. The interaction values are distributed symmetrically around zero, encompassing both positive and negative contributions, which demonstrates that the influence of individual features can shift depending on the conditions of a given transaction. This confirms that the model captures intricate dependencies among security parameters rather than treating each feature as an isolated contributor.

On the whole, the explainability results confirm that the proposed framework not only guarantees secure transaction verification but also delivers transparent and interpretable decision-making insights. In real-world scenarios where a transaction fails verification, the system is capable of pinpointing the primary contributing factors—such as an invalid blockchain confirmation or nonce reuse—enabling quicker

diagnosis and more effective regulatory auditing. This incorporation of explainable analytics strengthens stakeholder trust and promotes accountability within blockchain-based pharmaceutical supply chain systems.

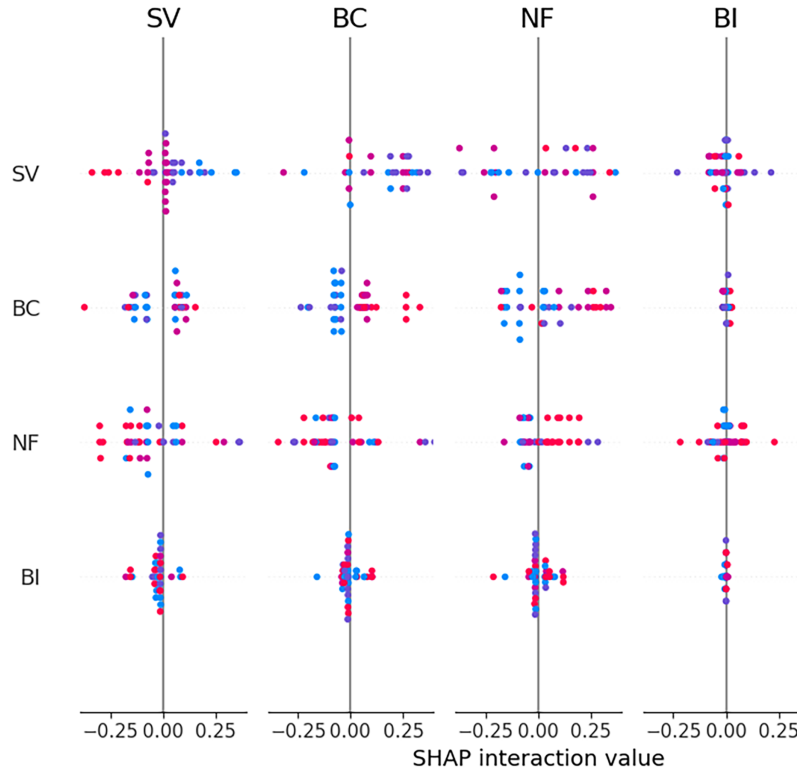


Figure 22: Pairwise SHAP interaction values revealing interdependencies among security verification features. The notably strong interaction observed between nonce freshness and signature verification demonstrates their synergistic role in upholding transaction security and reliability.

4.10 Transaction Verification Classification Performance

The classification performance of the proposed XAI-assisted verification model was further analyzed using confusion-matrix evaluation. Experimental results in Fig. 23 demonstrated stable classification performance with high interpretability consistency across repeated evaluations. The explainability outputs were then integrated with the blockchain audit layer to provide transparent and tamper-resistant verification reasoning. The Random Forest classifier achieved an average classification accuracy of 96.2%, with precision, recall, and F1-score values of 95.8%, 96.5%, and 96.1%, respectively. These results indicate stable and reliable transaction verification classification performance while maintaining high interpretability consistency across repeated experimental evaluations.

4.11 Comparative Discussion with Existing Research

When compared with recent blockchain-based healthcare supply-chain studies, the proposed framework demonstrates a balanced combination of security assurance, explainability, and practical computational efficiency. Existing studies such as Kumarswamy and Sampigerayappa [69] primarily focus on blockchain traceability and smart-contract deployment using Ethereum; however, they do not incorporate formal cryptographic verification or interpretable transaction validation mechanisms. Similarly, Ai et al. [70] proposed

an Ethereum-based traceable pharmaceutical framework achieving approximately 43 TPS with transaction latency around 2.5 s, but the architecture lacks explainability and protocol-level authentication guarantees.

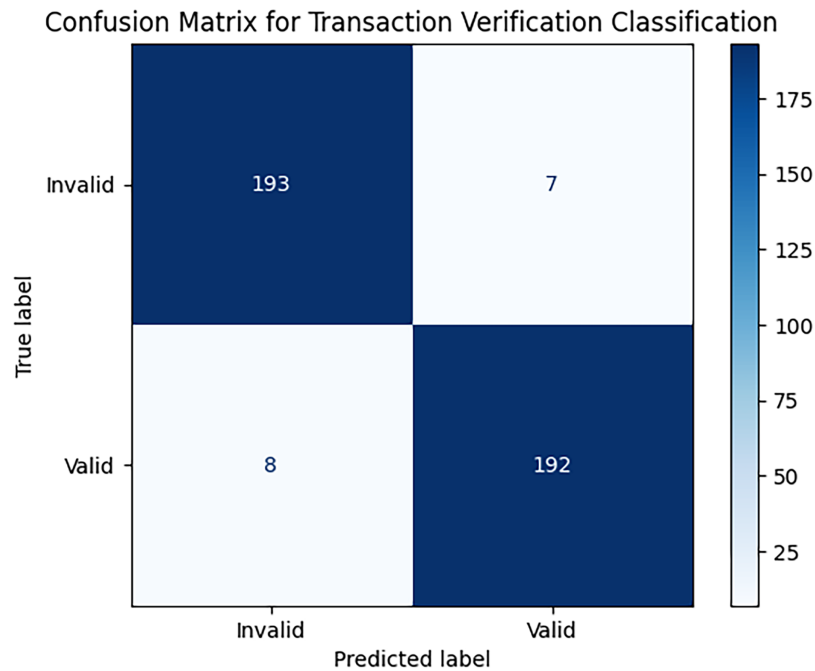


Figure 23: Confusion matrix of the proposed random forest-based transaction verification classifier demonstrating high classification accuracy for valid and malicious blockchain transactions.

Several Hyperledger Fabric-based studies report significantly higher throughput due to the permissioned nature of the Fabric architecture. Ganavi Urs et al. [71] and Aziz and Suman [72] demonstrated scalable healthcare supply-chain systems with throughput ranging from hundreds to thousands of transactions per second under benchmark conditions. However, these studies focus primarily on access control and distributed ledger management rather than formally verified authentication or explainable verification reasoning. Although Hyperledger Fabric and Ethereum employ different consensus and execution mechanisms, the comparison remains relevant because the proposed framework also operates within a permissioned private Ethereum environment configured for controlled healthcare deployment scenarios. Consequently, the comparison highlights architectural trade-offs between throughput optimization and integrated security transparency.

Renu and Gupta [73] further incorporated identity-management mechanisms into a Hyperledger-based healthcare architecture, improving authentication efficiency and scalability. Nevertheless, similar to most existing systems, the framework does not provide human-interpretable reasoning for security verification outcomes or mathematically validated protocol correctness.

Several studies emphasize that gas fees and transaction costs can become significant barriers to enterprise-scale blockchain adoption. Public Ethereum deployments often experience fluctuating gas costs and variable confirmation delays depending on network congestion and consensus overhead. In contrast, the proposed framework utilizes a lightweight permissioned Ethereum test environment with optimized smart-contract execution, resulting in predictable computational overhead and stable transaction latency during healthcare workload simulations. Additionally, the integration of formally verified cryptographic protocols

ensures that authentication integrity and replay-attack resistance are preserved without introducing excessive computational cost.

Another major distinction of the proposed framework lies in the integration of explainable verification mechanisms alongside blockchain authentication. While most existing healthcare blockchain systems primarily focus on traceability and immutable record management, comparatively fewer studies address the interpretability of security decisions. By integrating SHAP-based explainability with formally verified authentication, the proposed framework enables regulators and healthcare stakeholders to understand why transactions are accepted or rejected, thereby improving transparency, auditability, and operational trust. This architectural direction is further supported by Ressi et al. [61], who emphasized that future blockchain systems will increasingly incorporate AI-driven optimization, intelligent verification, and adaptive security mechanisms directly within decentralized infrastructures. The proposed framework aligns with this perspective by integrating explainable verification and intelligent transaction analysis into the blockchain-enabled healthcare supply-chain environment.

Overall, the experimental evaluation confirms that the proposed blockchain-enabled healthcare supply-chain architecture achieves secure and computationally efficient transaction processing while simultaneously providing formal security guarantees and explainable decision transparency. Table 4 demonstrates that the proposed framework extends beyond conventional blockchain traceability systems by integrating decentralized ledger security, formal cryptographic verification, and explainable transaction validation within a unified healthcare supply-chain architecture.

Table 4: Comparison of blockchain-based healthcare supply chain systems.

Reference	Blockchain Platform	Security Mechanism	Formal Verification	Explainability	TPS	Latency
Kumarswamy and Sampigerayappa [69] (2024)	Ethereum	Smart contracts + hashing	No	No	Not specified	Not specified
Ai et al. [70] (2022)	Ethereum	Smart contracts and distributed ledger	No	No	43 TPS	2.5 s
Ganavi Urs et al. [71] (2023)	Hyperledger Fabric	Access control + smart contracts	No	No	Up to 400 TPS (under load)	5–12 s
Aziz and Suman [72] (2024)	Hyperledger Fabric	Permissioned blockchain security	No	No	Up to 3000 TPS (benchmark test)	Variable
Renu and Gupta [73] (2025)	Hyperledger Fabric	Smart contracts + identity management	No	No	250 TPS	2.3 s
Proposed Framework	Ethereum private test network	Nonce-based authentication + digital signatures + smart contracts	Yes	Yes (SHAP-based XAI)	≈ 40 TPS	<3 s

Comparison with Alternative Digital Signature Schemes

To further evaluate the computational efficiency of the proposed authentication framework, the cryptographic signing overhead was compared with recent blockchain-oriented digital signature approaches

reported in contemporary healthcare and distributed ledger literature. The proposed framework employs elliptic-curve digital signatures due to their relatively low computational cost, compact key size, and suitability for lightweight blockchain environments.

Recent studies have explored alternative signature mechanisms including post-quantum signatures and hybrid encryption architectures for healthcare blockchain systems. Echikra et al. [74] demonstrated that ECDSA-based healthcare blockchain architectures maintain lower signing overhead and reduced storage complexity compared with heavyweight cryptographic alternatives. Similarly, Alsubai et al. [75] integrated anti-quantum cryptographic protection into blockchain-based healthcare systems, although the approach introduced additional computational overhead during transaction signing and verification. Schemitt et al. [76] further reported that post-quantum digital signature algorithms significantly increase transaction size and signing latency within blockchain environments.

Motivated by these observations, the proposed framework prioritizes lightweight elliptic-curve authentication mechanisms to maintain practical transaction throughput and scalable blockchain performance within pharmaceutical supply-chain environments. Table 5 summarizes the comparative characteristics of different blockchain-oriented digital signature approaches.

Table 5: Comparison of blockchain-oriented digital signature approaches used in recent healthcare and distributed ledger systems.

Approach	Signing Cost	Storage Overhead	Remarks
Healthcare IoRT ECDSA Framework [74]	Low	Moderate	Efficient authentication for interoperable healthcare blockchain systems
Hybrid Encryption with Anti-Quantum Signatures [75]	Moderate-High	Moderate	Enhanced security with additional computational overhead
Post-Quantum Signature Schemes [76]	High	High	Improved quantum resistance but increased transaction latency
Proposed Framework	Low	Low	Lightweight and suitable for scalable healthcare blockchain deployment

The comparative analysis indicates that lightweight elliptic-curve cryptographic mechanisms remain more practical for scalable pharmaceutical blockchain deployments when compared with computationally intensive post-quantum alternatives. Although post-quantum cryptography provides stronger future-oriented security guarantees, current blockchain healthcare environments continue to prioritize computational efficiency, low latency, and reduced storage overhead for large-scale deployment scenarios.

4.12 Ablation Study

An ablation study was conducted to evaluate the contribution of individual framework components including blockchain traceability, formal cryptographic verification, and SHAP-based explainability. The

objective of the analysis was to determine how each module contributes to overall system security, interpretability, and transaction traceability within the pharmaceutical supply-chain environment. The study evaluates four experimental configurations by selectively removing major framework components:

- Without Blockchain
- Without XAI
- Without Formal Verification
- Full Proposed Framework

The evaluation metrics were derived from experimental protocol validation results, explainability performance, and blockchain transaction verification outcomes obtained during the simulated healthcare supply-chain experiments. Security score represents successful resistance against replay, impersonation, and unauthorized transaction attacks. Interpretability score reflects the quality of transaction-level explanation generated by the SHAP-based verification module, while traceability score measures the ability to securely track and verify pharmaceutical transactions across the blockchain ledger. For quantitative comparison, each evaluation metric was normalized to a percentage scale between 0 and 100 based on experimental observations obtained during protocol verification, blockchain transaction analysis, and explainability evaluation. The security score was derived from successful resistance against replay attacks, impersonation attempts, unauthorized transaction submissions, and authentication failures during adversarial simulation experiments. The interpretability score was computed using explanation consistency, feature-attribution stability, and human-readable verification transparency generated by the SHAP-based explainability module. The traceability score measured successful end-to-end transaction tracking, blockchain audit consistency, and immutable verification performance across distributed supply-chain participants. Final scores were obtained by averaging normalized results across repeated experimental runs under varying transaction workloads and adversarial conditions.

The results demonstrate in [Table 6](#) that removing blockchain functionality significantly reduces transaction traceability and overall system integrity. Excluding the XAI module substantially decreases interpretability because stakeholders no longer receive transparent explanations regarding transaction verification decisions. Similarly, removing formal verification weakens protocol-level security assurance by eliminating mathematical validation of authentication correctness under adversarial conditions. The reported scores were normalized from aggregated experimental measurements obtained during protocol validation, SHAP explainability evaluation, replay-attack detection experiments, and blockchain transaction-verification analysis. Each metric was scaled to a percentage-based comparative score to enable relative evaluation among different framework configurations.

Table 6: Ablation study comparing the contribution of blockchain, explainability, and formal verification components in the proposed framework.

Configuration	Security Score (%)	Interpretability (%)	Traceability (%)
Without Blockchain	71.2	42.0	38.4
Without XAI	80.5	10.0	83.1
Without Formal Verification	84.3	45.2	82.7
Full Proposed Framework	96.8	94.5	97.2

The complete integrated framework achieved the highest overall performance by combining decentralized blockchain traceability, formally verified authentication, and explainable security analytics within

a unified architecture. These findings confirm that each framework component contributes significantly to secure, transparent, and trustworthy pharmaceutical supply-chain operations.

5 Conclusion

This study presented a unified blockchain-enabled healthcare drug supply-chain framework integrating formally verified cryptographic authentication, decentralized blockchain traceability, Solidity smart contracts, and SHAP-based explainable security verification. The proposed architecture combines nonce-based challenge-response authentication, elliptic-curve digital signatures, smart-contract-driven transaction validation, and blockchain-based immutable logging to establish secure and tamper-resistant pharmaceutical supply-chain operations. Formal verification using ProVerif confirmed that the protocol preserves secrecy, authentication, integrity, and replay-attack resistance under the symbolic Dolev-Yao adversarial model, with no executable attack traces identified during verification. Beyond symbolic analysis, implementation-level validation was additionally performed through Mythril-based static smart-contract security auditing and successful deployment within the Ethereum Sepolia test network, further demonstrating the practical robustness and deployability of the proposed framework beyond isolated local simulation environments. Experimental evaluation demonstrated efficient computational performance, including average cryptographic signing latency of approximately 0.71 ms per transaction, stable blockchain transaction latency below 3 s, predictable near-linear storage scalability, and manageable gas-consumption overhead under increasing transaction workloads. Throughput, scalability, and fault-tolerance analyses additionally confirmed stable operational behavior under increasing node participation and heterogeneous transaction conditions, indicating the suitability of the proposed framework for secure healthcare logistics environments.

A major contribution of this work lies in integrating explainable artificial intelligence into blockchain-based healthcare security verification. Unlike conventional cryptographic verification systems that provide binary acceptance decisions without interpretability, the proposed SHAP-based explanation layer identifies the relative contribution of security features such as signature validity, nonce freshness, blockchain confirmation, and transaction integrity verification toward final transaction-validation outcomes. The explainability module further achieved strong classification consistency during transaction-verification evaluation, with the Random Forest classifier obtaining approximately 96.2% accuracy together with low false-classification behavior across simulated adversarial transaction scenarios. These capabilities improve transparency, auditability, stakeholder trust, and regulatory oversight within healthcare supply chains. Comparative evaluation and ablation analysis additionally demonstrated that combining blockchain infrastructure, formal verification, and explainable analytics provides stronger overall security assurance, interpretability, and traceability than standalone blockchain architectures. From an engineering and deployment perspective, the proposed framework contributes a reproducible, extensible, and privacy-aware architecture capable of supporting secure pharmaceutical traceability, decentralized verification, interpretable compliance auditing, and transparent transaction management within modern healthcare ecosystems.

Despite these contributions, several practical deployment challenges remain. The current evaluation was conducted within a controlled permissioned Ethereum test environment using synthetically generated workload traces rather than real industrial healthcare infrastructures. Although synthetic workloads improve reproducibility while preserving privacy and regulatory constraints, real-world pharmaceutical ecosystems may exhibit additional behavioral variability, operational heterogeneity, and large-scale network dynamics not fully captured within controlled simulation environments. Large-scale deployment across geographically distributed healthcare infrastructures may also introduce constraints related to interoperability between heterogeneous blockchain platforms, dynamic consensus overhead, cloud-edge synchronization, regulatory compliance, infrastructure maintenance cost, and enterprise-level operational management. While

Mythril-based static analysis did not identify critical vulnerabilities such as reentrancy conditions or integer-overflow risks within the implemented smart contracts, additional runtime-oriented attack surfaces and deployment-specific security challenges may still emerge under complex real-world operational environments. Future research will therefore focus on large-scale distributed deployment evaluation, integration of advanced runtime monitoring and dynamic smart-contract auditing techniques, incorporation of privacy-preserving mechanisms such as zero-knowledge proofs and secure multi-party computation, and exploration of AI-enhanced blockchain optimization strategies for intelligent compliance management and adaptive transaction orchestration. These extensions would further strengthen the practical deployment readiness, scalability, transparency, and regulatory trustworthiness of blockchain-enabled healthcare drug supply-chain systems operating within real-world pharmaceutical environments.

Acknowledgement: Not applicable.

Funding Statement: This research received no external funding.

Author Contributions: The authors declare their individual contributions to this paper as follows: Muammar Shahrear Famous: Conceptualization, methodology, visualization, writing—review and editing; Samia Sayed: Conceptualization, data curation, formal analysis, investigation, writing—original draft; Rashed Mazumder: Methodology, validation, investigation, writing—original draft; Risala T. Khan: Data curation, formal analysis, validation, writing—original draft; M. Shamim Kaiser: Resources, supervision, writing—review and editing; Mohammad Shahadat Hossain: Project administration, supervision, methodology; Karl Andersson: Conceptualization, project administration, supervision, writing—review and editing. All authors reviewed and approved the final version of the manuscript.

Availability of Data and Materials: The original contributions presented in this study are included in the article. The prototype implementation, Solidity smart contracts, ProVerif models, experimental scripts, and evaluation datasets are available from the corresponding author upon reasonable academic request.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Kumar P, Mohammad G, Narsimhulu P, Narasappa D, Maguluri L, Singh S, et al. Computer modeling approaches for blockchain-driven supply chain intelligence: a review on enhancing transparency, security, and efficiency. *Comput Model Eng Sci.* 2025;144(3):2779–818.
2. Kaviyasri S, Jayasri RB, Rajarajeswari C, Jaipriya S. A blockchain and edge computing approach to ensure drug authenticity and safety. In: 2026 Second International Conference on Intelligent Systems for Communication, IoT and Security (ICISCOIS); 2026 Jan 7–9; Coimbatore, India. Piscataway, NJ, USA: IEEE; 2026. p. 1–6.
3. Sayed S, Famous MS, Mazumder R, Khan RT, Kaiser MS, Hossain MS, et al. Blockchain and InterPlanetary framework for decentralized and secure electronic health record management. *Blockchains.* 2025;3(4):12. doi:10.3390/blockchains3040012.
4. Arslanoğlu K, Karaköse M. An overview for trustworthy and explainable artificial intelligence in healthcare. In: 2024 28th International Conference on Information Technology (IT); 2024 Feb 21–24; Žabljak, Montenegro. Piscataway, NJ, USA: IEEE; 2024. p. 1–5.
5. Rupa C, Varshitha GS, Divya D, Gadekallu TR, Piran MJ. Blockchain-based DApp for drug supply chain with AI-driven drug recommender system. *IEEE Consum Electron Mag.* 2025;15(1):1–6. doi:10.1109/mce.2025.3536326.
6. Abbas K, Afaq M, Khan TA, Song WC. A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry. *Electronics.* 2020;9(5):852. doi:10.3390/electronics9050852.

7. Alsagheer D, Xu L, Shi W. Decentralized machine learning governance: overview, opportunities, and challenges. *IEEE Access*. 2023;11:96718–32.
8. Charles V, Emrouznejad A, Gherman T. A critical analysis of the integration of blockchain and artificial intelligence for supply chain. *Ann Oper Res*. 2023;327(1):7–47. doi:10.1007/s10479-023-05169-w.
9. Pathak R, Gaur V, Sankrityayan H, Gogtay J. Tackling counterfeit drugs: the challenges and possibilities. *Pharmaceut Med*. 2023;37(4):281–90. doi:10.1007/s40290-023-00468-w.
10. Ahmadi V, Benjelloun S, El Kik M, Sharma T, Chi H, Zhou W. Drug governance: IoT-based blockchain implementation in the pharmaceutical supply chain. In: 2020 Sixth International Conference on Mobile and Secure Services (MobiSecServ); 2020 Feb 22–23; Miami Beach, FL, USA. Piscataway, NJ, USA: IEEE; 2020. p. 1–8.
11. Singh R, Dwivedi AD, Srivastava G. Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. *Sensor*. 2020;20(14):3951.
12. Omar IA, Debe M, Jayaraman R, Salah K, Omar M, Arshad J. Blockchain-based supply chain traceability for COVID-19 personal protective equipment. *Comput Ind Eng*. 2022;167:107995. doi:10.1016/j.cie.2022.107995.
13. Cui L, Xiao Z, Chen F, Dai H, Li J. Protecting vaccine safety: an improved, blockchain-based, storage-efficient scheme. *IEEE Trans Cybern*. 2023;53(6):3588–98.
14. Amoozad Mahdiraji H, Yaftiyan F, Abbasi-Kamardi A, Garza-Reyes JA. Investigating potential interventions on disruptive impacts of industry 4.0 technologies in circular supply chains: evidence from SMEs of an emerging economy. *Comput Ind Eng*. 2022;174(2):108753. doi:10.1016/j.cie.2022.108753.
15. Kumar V, Das SK. Enhancing security in IIoT: RFID authentication protocol for edge computing and blockchain-enabled supply chain. *Cyber Secur Appl*. 2025;3:100087.
16. Liu L, Song W, Liu Y. Leveraging digital capabilities toward a circular economy: reinforcing sustainable supply chain management with industry 4.0 technologies. *Comput Ind Eng*. 2023;178:109113.
17. Crossland V, Dellwo C, Bashar G, Dagher GG. Janus: toward preventing counterfeits in supply chains utilizing a multi-quorum blockchain. *Blockchain: Res Appl*. 2023;4(4):100157.
18. Agrawal K, Aggarwal M, Tanwar S, Alabdulatif A. Adoption of blockchain to develop a deployable secure healthcare solution: an analysis. *Cyber Secur Appl*. 2024;3(10):100060. doi:10.1016/j.csa.2024.100060.
19. Chen X, He C, Chen Y, Xie Z. Internet of things (IoT)—blockchain-enabled pharmaceutical supply chain resilience in the post-pandemic era. *Front Eng Manag*. 2023;10(1):82–95. doi:10.1007/s42524-022-0233-1.
20. Sayed S, Shahrear Famous M, Mazumder R, Khan RT, Shamim Kaiser M, Hossain MS, et al. Secure health record management system with blockchain and local storage integration. In: Mahmud M, Kaiser MS, Bandyopadhyay A, Ray K, Bunde M, editor. *Proceedings of Trends in Electronics and Health Informatics*. Singapore: Springer Nature Singapore; 2026. p. 133–50.
21. Sayed S, Shahrear Famous M, Ahammad S, Hossain T, Khan RT, Kaiser MS. Toward distributed security based healthcare system. In: Kaiser MS, Singh R, Bandyopadhyay A, Mahmud M, Ray K, editor. *Proceedings of the Fifth International Conference on Trends in Computational and Cognitive Engineering*. Singapore: Springer Nature; 2024. p. 445–58.
22. Altigani A, Hasan S, Barry B, Naserelden S, Elsadig MA, Elshoush HT. A polymorphic advanced encryption standard—a novel approach. *IEEE Access*. 2021;9:20191–207. doi:10.1109/access.2021.3051556.
23. Booher DD, Cambou B, Carlson AH, Philabaum C. Dynamic key generation for polymorphic encryption. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019; 2019 Jan 7–9; Las Vegas, NV, USA. Piscataway, NJ, USA: IEEE; 2019. p. 482–7.
24. Meng Y, Li J. Data sharing mechanism of sensors and actuators of industrial IoT based on blockchain-assisted identity-based cryptography. *Sensors*. 2021;21(18):6084.
25. Shim KA, An Y. Cryptanalysis of lattice-based blind signature and blind ring signature schemes. *IEEE Access*. 2021;9:134427–34. doi:10.1109/access.2021.3113938.
26. Simion E. Encapsulating secrets using lockable obfuscation and a RMERS-based public key encryption. *Sustainability*. 2022;14(18):11412. doi:10.3390/su141811412.
27. Xie J, Zhao W, Lee H, Roy DB, Zhang X. Hardware circuits and systems design for post-quantum cryptography—a tutorial brief. *IEEE Trans Circuits Syst II: Exp Briefs*. 2024;71(3):1670–6. doi:10.1109/tcsii.2024.3357836.

28. Kim S. Optimized SeaSign for enhanced efficiency. *IEEE Access*. 2024;12:18851–7. doi:10.1109/access.2024.3360297.
29. Dashtizadeh M, Meskaran F, Tan D. A secure blockchain-based pharmaceutical supply chain management system: traceability and detection of counterfeit COVID-19 vaccines. In: 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon); 2022 Oct 16–17; Mysuru, India. Piscataway, NJ, USA: IEEE; 2022. p. 1–5.
30. Debe M, Salah K, Jayaraman R, Arshad J. Blockchain-based verifiable tracking of resellable returned drugs. *IEEE Access*. 2020;8:205848–62. doi:10.1109/access.2020.3037363.
31. Musamih A, Jayaraman R, Salah K, Hasan HR, Yaqoob I, Al-Hammadi Y. Blockchain-based solution for distribution and delivery of COVID-19 vaccines. *IEEE Access*. 2021;9:71372–87. doi:10.1109/access.2021.3079197.
32. Musamih A, Jayaraman R, Salah K, Hasan HR, Yaqoob I, Al-Hammadi Y. Blockchain-based solution for the administration of controlled medication. *IEEE Access*. 2021;9:145397–414. doi:10.1109/access.2021.3121545.
33. Mohit M, Kaur S, Singh M. Design and implementation of transaction privacy by virtue of ownership and traceability in blockchain based supply chain. *Cluster Comput*. 2022;25(3):2223–40. doi:10.1007/s10586-021-03425-x.
34. Saindane P, Jethani Y, Mahtani P, Rohra C, Lund P. Blockchain: a solution for improved traceability with reduced counterfeits in supply chain of drugs. In: 2020 International Conference on Electrotechnical Complexes and Systems (ICOECS); 2020 Oct 27–30; Ufa, Russia. Piscataway, NJ, USA: IEEE; 2020. p. 1–5.
35. Marbough D, Abbasi T, Maasmi F, Omar IA, Debe MS, Salah K, et al. Blockchain for COVID-19: review, opportunities, and a trusted tracking system. *Arab J Sci Eng*. 2020;45(12):9895–911. doi:10.1007/s13369-020-04950-4.
36. Famous MS, Sayed S, Mazumder R, Khan RT, Shamim Kaiser M, Hossain MS, et al. PharmaShield: optimized blockchain framework for pharma supply. In: 2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS); 2025 Oct 23–24; Kushtia, Bangladesh. Piscataway, NJ, USA: IEEE; 2025. p. 1–12.
37. Chang SE, Chen Y. When blockchain meets supply chain: a systematic literature review on current development and potential applications. *IEEE Access*. 2020;8:62478–94.
38. Sahoo M, Singhar SS, Nayak B, Mohanta BK. A blockchain based framework secured by ECDSA to curb drug counterfeiting. In: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT); 2019 Jul 6–8; Kanpur, India. Piscataway, NJ, USA: IEEE; 2019. p. 1–6.
39. Jamil F, Hang L, Kim K, Kim DH. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. *Electronics*. 2019;8(5):505. doi:10.3390/electronics8050505.
40. Pham HL, Tran TH, Nakashima Y. Practical anti-counterfeit medicine management system based on blockchain technology. In: 2019 4th Technology Innovation Management and Engineering Science International Conference (TIMES-iCON); 2019 Dec 11–13; Bangkok, Thailand. Piscataway, NJ, USA: IEEE; 2019. p. 1–5.
41. He Q, He H. A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining. *Sustainability*. 2021;13(1):101. doi:10.3390/su13010101.
42. Mani V, Prakash M, Lai WC. Cloud-based blockchain technology to identify counterfeits. *J Cloud Comp*. 2022;11(1):67. doi:10.1186/s13677-022-00341-2.
43. Xu Z, Luo M, Peng C, Feng Q. Sanitizable signature scheme with privacy protection for electronic medical data sharing. *Cyber Secur Appl*. 2023;1(16):100018. doi:10.1016/j.csa.2023.100018.
44. Sowjanya Y, Gopalakrishnan S, Kumar RD. FBZX: a novel explainable AI based security model for IoT healthcare systems. In: 2025 Third International Conference on Augmented Intelligence and Sustainable Systems (ICAISS); 2025 May 21–23; Trichy, India. Piscataway, NJ, USA: IEEE; 2025. p. 106–10.
45. Murthy CVNUB, Shri ML. Novel architecture integrating XAI with blockchain and IoT devices for healthcare. In: 2024 Second International Conference on Emerging Trends in Information Technology and Engineering (ICETITE); 2024 Feb 22–23; Vellore, India. Piscataway, NJ, USA: IEEE; 2024. p. 1–5.
46. Dutta J, Puthal D. Advancing eHealth in society 5.0: a fuzzy logic and blockchain-enhanced framework for integrating IoMT, edge, and cloud with AI. *IEEE Access*. 2024;12:195710–30.

47. Dutta J, Eldeeb HB, Ho TD. Advanced eHealth with explainable AI: secured by blockchain with AI-empowered block sensitivity for adaptive authentication. In: 2024 IEEE 35th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC); 2024 Sep 2–5; Valencia, Spain. Piscataway, NJ, USA: IEEE; 2024. p. 1–7.
48. Ali S, Abdullah, Armand TPT, Athar A, Hussain A, Ali M, et al. Metaverse in healthcare integrated with explainable AI and blockchain: enabling immersiveness, ensuring trust, and providing patient data security. *Sensors*. 2023;23(2):565.
49. Mavrogiorgos K, Gur S, Kalantzis N, Tzelapsis K, Papageorgiou XS, Karabetian A, et al. Combining explainable artificial intelligence (XAI) with blockchain towards trustworthy data-driven policies. In: 2025 21st International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT); 2025 Jun 9–11; Tuscany, Italy. Piscataway, NJ, USA: IEEE; 2025. p. 1042–9.
50. Njoku JN, Nwakanma CI, Lee JM, Kim DS. Trustworthy battery management: a digital twin approach leveraging XAI and blockchain. In: 2025 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC); 2025 Feb 18–21; Fukuoka, Japan. Piscataway, NJ, USA: IEEE; 2025. p. 0448–53.
51. Wang X, Ye D, Feng C, Yang HH, Chen X, Quek TQS. Trustworthy image semantic communication with GenAI: explainability, controllability, and efficiency. *IEEE Wirel Commun*. 2025;32(2):68–75. doi:10.1109/mwc.001.2400304.
52. Rathod T, Jadav NK, Tanwar S, Polkowski Z, Yamsani N, Sharma R, et al. AI and blockchain-based secure data dissemination architecture for IoT-enabled critical infrastructure. *Sensors*. 2023;23(21):8928. doi:10.3390/s23218928.
53. Gadekallu TR, Kumar Reddy Maddikunta P, Boopathy P, Deepa N, Chengoden R, Victor N, et al. XAI for industry 5.0—concepts, opportunities, challenges, and future directions. *IEEE Open J Commun Soc*. 2025;6(11):2706–29. doi:10.1109/ojcoms.2024.3473891.
54. Hasan M, Rahman MS, Morshed Chowdhury MJ, Sarker IH. CNN based deep learning modeling with explainability analysis for detecting fraudulent blockchain transactions. *Cyber Secur Appl*. 2025;3(3):100101. doi:10.1016/j.csa.2025.100101.
55. Hasan M, Rahman MS, Janicke H, Sarker IH. Detecting anomalies in blockchain transactions using machine learning classifiers and explainability analysis. *Blockchain Res Appl*. 2024;5(3):100207. doi:10.1016/j.bcr.2024.100207.
56. Kritika E. A comprehensive literature review on ransomware detection using deep learning. *Cyber Secur Appl*. 2025;3(2):100078. doi:10.1016/j.csa.2024.100078.
57. Zhang Y, Wu M, Zhang G, Lu J. Responsible AI: portraits with intelligent bibliometrics. *IEEE Trans Artif Intell*. 2025;6(8):1977–90.
58. Bonnet S, Di Francesco Maesa D, Loporchio M, Tietze F. A fair and trustworthy remuneration framework for AI model training using DLT. In: 2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC); 2025 Jun 2–6; Pisa, Italy. Piscataway, NJ, USA: IEEE; 2025. p. 1–5.
59. Al Ghanmi H, Bahsoon R. ExplanaSC: a framework for determining information requirements for explainable blockchain smart contracts. *IEEE Trans Softw Eng*. 2024;50(8):1984–2004.
60. Bistarelli S, Faloci F, Mori P. *-chain: a framework for automating the modeling of blockchain based supply chain tracing systems. *Future Gener Comput Syst*. 2023;149:679–700.
61. Ressi D, Romanello R, Piazza C, Rossi S. AI-enhanced blockchain technology: a review of advancements and opportunities. *J Netw Comput Appl*. 2024;225:103858.
62. Madupati B, Jonnalagadda AK, Vududala SK, Vegesna RV. Federated learning meets data engineering: building trustworthy AI with decentralized data pipelines. In: 2025 International Conference on Computing Technologies (ICOCT); 2025 Jun 13–14; Bengaluru, India. Piscataway, NJ, USA: IEEE; 2025. p. 1–7.
63. Pavlova E, Melnikov G, Yanovich Y, Frolov A. Unlocking potential of open source model training in decentralized federated learning environment. *Blockchain Res Appl*. 2025;6(2):100264. doi:10.1016/j.bcr.2024.100264.
64. Mu J, Kadoch M, Yuan T, Lv W, Liu Q, Li B. Explainable federated medical image analysis through causal learning and blockchain. *IEEE J Biomed Health Inform*. 2024;28(6):3206–18. doi:10.1109/jbhi.2024.3375894.

65. Kumar A, Mani V, Jain V, Gupta H, Venkatesh VG. Managing healthcare supply chain through artificial intelligence (AI): a study of critical success factors. *Comput Ind Eng.* 2023;175:108815.
66. Korde N, Diwan T, Digalwar M. An iterative systematic analytical review of machine learning techniques for blockchain optimization. *IEEE Access.* 2025;13(1):156021–44. doi:10.1109/access.2025.3604287.
67. Potdukhe N, Gourshettiwar P, Zade S, Waghale A. Blockchain-enabled federated learning systems with explainable AI: a review. In: 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS); 2025 Mar 10–12; Bangkok, Thailand. Piscataway, NJ, USA: IEEE; 2025. p. 1650–6.
68. Vimbi V, Shaffi N, Mahmud M. Interpreting artificial intelligence models: a systematic review on the application of LIME and SHAP in Alzheimers disease detection. *Brain Inform.* 2024;11(1):10.
69. Kumarswamy S, Sampigerayappa PA. Leveraging blockchain technology to establish a transparent and counterfeit-resistant pharmaceutical supply chain. *J Eur Syst Autom.* 2024;57(5):1429–43. doi:10.18280/jesa.570518.
70. Ai Y, Chen CL, Weng W, Chiang ML, Deng YY, Lim ZY. A traceable vaccine supply management system. *Sensors.* 2022;22(24):9670. doi:10.3390/s22249670.
71. Ganavi Urs BL, Sushitha AS, Vibha Shree MS, Prathima M, Arpitha MS. Traceability of counterfeit medicine supply chain through blockchain. In: Hiranwal S, Mathur G, editors. *Artificial intelligence and communication technologies.* New Delhi, India: SCRS; 2023. p. 1003–7. doi:10.52458/978-81-955020-5-9-95.
72. Aziz A, Suman S. Development of a blockchain-based system for drug counterfeiting and traceability in the pharmaceutical supply chain. *Res Rev.* 2024;15(3):99–114. doi:10.37591/rrjops.v15i03.186127.
73. Renu SA, Gupta A. A blockchain-IoT framework for preventing counterfeit medical supplies via ride-sharing networks. *J Eur Syst Autom.* 2025;58(2):225–36. doi:10.18280/jesa.580204.
74. Echikra A, Yachira A, Kerracheb CA, Sahraoui Z. ECDSA-secured blockchain architecture for interoperable healthcare in the internet of robotic things (IoRT). *Inf Secur J: Glob Perspect.* 2026;35(1):53–64. doi:10.1080/19393555.2024.2399515.
75. Alsubai S, Alqahtani A, Garg H, Sha M, Gumaei A. A blockchain-based hybrid encryption technique with anti-quantum signature for securing electronic health records. *Complex Intell Syst.* 2024;10(5):6117–41. doi:10.1007/s40747-024-01477-1.
76. Schemitt AG, Silva HFd, Lunardi RC, Kreutz D, Mansilha RB, Zorzo AF. Assessing the impact of post-quantum digital signature algorithms on blockchains. *arXiv:2510.09271.* 2025.