Natural Resources for Human Health

eISSN: 2583-1194

Original Research

Received 22 July 2026
Revised 24 Aug 2026
Accepted 05 Sep 2026

Natural Resources for Human Health 2026, Vol.6(22s):1003–1020

KEYWORDS:
pharmaceutical supply chain, blockchain, traceability, counterfeit medicines, security, privacy, zero-knowledge proofs, self-sovereign identity, smart contracts, IPFS, IoT, effectiveness evaluation.

Security, Privacy, and Effectiveness Evaluation of Blockchain-based Pharmaceutical Traceability through Comparative Analysis with State-of-the-Art Approaches

Nida Khan[1]*, Dr. Mohammad Suaib[2]

[1]Computer Science & Engineering, Integral University, Lucknow, India
[2]Computer Science & Engineering, Integral University, Lucknow, India
[1]nidahadihasan@gmail.com, [2]suaibcs09@gmail.com

ABSTRACT:

Pharmaceutical supply chains rely on trustworthy provenance, rapid verification, selective disclosure, and operationally useful traceability across manufacturers, distributors, logistics providers, pharmacies, healthcare institutions, regulators, and patients. Main databases, barcode/QR recognition, RFID, and enterprise systems provide useful tracking, however, they could remain fragmented, centrally dependent, difficult to audit over organizational borders, or vulnerable to weak data provenance. A recent study from 2025-2026 has shown that the blockchain is increasingly being combined with permissioned governance, off-chain storage, modern signatures, SSI, ZKPs, IoT, NFC, big-data analytics, and decentralized storage. This conceptual paper synthesizes all those state-of-the-art directions and proposes a unified evaluation framework for security, privacy, and effectiveness, rather than considering blockchain adoption itself as evidence of improvement.

The paper proposes that the pharmaceutical traceability should be viewed as a socio-technical system. Immutability of the ledger protects information once recorded, but it does not guarantee that the original event was true. Pseudonymous blockchain addresses cannot imply privacy. Effectiveness depends on throughput, latency, speed of recall, counterfeit detection ability, quality of data, interoperability, usability and governance. The suggested conceptual architecture thus separates identity, event evidence, transaction state, detailed records, and analytics, bound through verifiable cryptographic commitments with policy-controlled access. In this paper, we propose a comparative rubric to assess centralized, QR/RFID, conventional blockchain, blockchain-plus-IPFS/cloud, blockchain-plus-SSI/ZKP, and emerging DAG/NFC approaches. Under the framework, expected to provide guidance for the implementation of future prototypes and empirical benchmarking, performance will not be fabricated at a conceptual stage. The help of blockchain technology in the pharmaceutical supply chain can ensure the delivery of authentic financial goods.

1. INTRODUCTION

Pharmaceutical traceability is more of a critical information safety problem than an inventory management one. A medicine can pass through raw-material providers, manufacturing sites, contract manufacturers, QA labs, warehouses, distributors, transport operatives, pharmacies, hospitals, and patients. At every transition, an organization should be capable of specifying what was handled, by whom, when and under what conditions, and whether the corresponding evidence can be trusted. As a result, incidents of various counterfeit activities can endanger the supply chain and public health. Blockchain is appealing as a distributed ledger can provide a common, tamper-evident record of transactions among organizations that do not fully trust

each other. Studies indicate, however, that the value of a blockchain depends strongly on its governance, permissioning, data placement, identity management, and the quality of the evidence added to the ledger. A 2026 mapping review of 103 records found rapid growth in pharmaceutical blockchain research but also emphasized heterogeneous technical rigor and inconsistent formalization of chain-of-custody semantics and evaluation methods [1]. According to a study in 2025 that analyzed empirical evidence, they found that IT security again featured as a major challenge towards adoption. Furthermore, they highlight organizational, regulatory, and training countermeasures. [2]

As a result, the state of the art is evolving past blockchain-only solutions. Recent approaches use blockchain technologies in combination with Hyperledger Fabric or Ethereum, off-chain storage like IPFS or cloud storage, EdDSA signatures, SSI, ZKPs, big data analytics and sensor technologies. Recent work advocates for storing records on the blockchain with IPFS links to reduce on-chain storage, SSI-enabled vaccine traceability to improve identity privacy, ZKP-enabled recall workflows to support selective disclosure, and DAG/NFC design to enable lower-latency edge authentication [3–7].

In the literature, studies are found that evaluate a particular architecture, cryptographic primitive or prototype. But fewer papers give a common conceptual rubric that assesses security, privacy and operational effectiveness against state-of-the-art security alternatives. Here, we do not want to suggest that one architecture has already been proven better. The paper however defines what is to be measured, what trade-offs to consider, and how a future experimental implementation can produce comparable evidence.

1.1 Objectives

- A security model for the traceability of pharmaceuticals covering authenticity, integrity, non-repudiation, availability, insertion of counterfeits, replay, impersonation, key compromise, smart-contract, and IoT and Governance threats.
- Set out privacy parameters for supply-chain data that is business-sensitive; for stakeholder identity, transaction metadata, patient-facing verification, and regulatory disclosure.
- Establish a framework to track and trace vaccine attributes which covers recall responsiveness, counterfeit-detection capability, throughput, latency, storage, cost, interoperability, and usability.
- Evaluate top approaches using a clear standardized scoring system, and identify falsifiable research questions.
- The accompanying paper would detail at least one modular architecture that integrates permissioned blockchain, cryptographic commitments, off-chain encrypted storage, SSI/ZKP, IoT/NFC evidence, analytics.

2. Pharmaceutical Traceability: Problem Structure and Requirements

To be effective, traceability should allow us to maintain a chain from creation to final verification. Core units may be serialized packages, batches, pallets, shipments or aggregation hierarchy. Each unit shall have, unique identification, origin event, manufacturing event, quality event, custody transfer event, environmental observation(s), verification event or disposition event. the information model must differentiate between the physical product and its digital counterpart. An immutable record merely preserves an incorrect association between the real product and the counterfeit cyber product.

2.1 Functional specifications

- Identity and authorization: only accredited participants and approved devices should create privileged events.
- Provenance: each material, batch, or serialized product should have a verifiable history.
- Event integrity: modifications to recorded evidence should be detectable.
- Selective verification: a verifier should be able to confirm authenticity without receiving unnecessary commercial or personal information.
- Recall support: affected products should be locatable quickly and the responsible custody chain should be auditable.
- Condition monitoring: temperature, humidity, shock, location, and handling events should be linked to the appropriate shipment or product where required.
- Interoperability: traceability records should connect to ERP, warehouse, serialization, health-information, customs, and regulatory systems.
- Exception handling: the system must represent returns, quarantine, destruction, expiry, recalls, corrections, and disputed events rather than assuming a perfect linear chain.

2.2 Non-functional requirements

Security and privacy are necessary but not sufficient. A practical pharmaceutical platform must also be scalable, available, economically sustainable, usable by heterogeneous organizations, and compatible with regulatory requirements. The 2025 literature emphasizes that permissioned and private networks are common because pharmaceutical supply chains require controlled participation and confidential information, while off-chain storage is frequently used to reduce ledger burden [8].

Requirement	Meaning for pharmaceutical traceability	Indicative metric
Security	Resistance to tampering, impersonation, replay and unauthorized actions	attack success rate; verification failure rate
Privacy	Minimum necessary disclosure of identity and business/patient information	data exposure; linkability; disclosure volume
Traceability	Completeness and correctness of custody/event history	traceability completeness (%)
Effectiveness	Ability to detect, verify, recall and audit medicines	verification accuracy; recall time
Performance	Operational responsiveness at realistic workload	throughput; latency; CPU/network load
Scalability	Growth across participants, products, sensors and events	transactions/s; storage growth
Interoperability	Exchange with existing systems and standards	successful interface transactions (%)
Governance	Controlled onboarding, roles, dispute and revocation processes	policy coverage; recovery time

3. State-of-the-Art Approaches (2025–2026)

Recent work demonstrates a shift from basic blockchain traceability to layered, privacy-sensitive, cryptographic and more robust architectures. The following methods will be considered design families rather than technologies.

Approach	Representative direction	Primary strength	Principal limitation
Centralized/ERP database	Conventional enterprise track-and-trace	Mature integration and high query performance	Single administrative trust domain; cross-organization provenance is harder to establish
QR/barcode serialization	Package-level consumer or distributor verification	Low cost and broad device compatibility	Code cloning and weak binding to physical product unless protected by stronger mechanisms
RFID/IoT traceability	Automated sensing and identification	Real-time condition and movement evidence	Device compromise, connectivity, sensor trust and privacy issues
Permissioned blockchain	Hyperledger Fabric / consortium ledger	Shared audit trail with controlled participation	Governance complexity and ledger-performance constraints
Blockchain + IPFS/cloud	On-chain commitments with off-chain detailed records	Reduced on-chain storage and auditable data integrity	Off-chain confidentiality, availability and deletion/governance must be managed separately
Blockchain + EdDSA	Modern digital signatures for drug events	Efficient authentication and resource use	Does not by itself solve privacy, identity governance or truthful data capture
Blockchain + SSI	Decentralized identity and verifiable credentials	Portable identity and fine-grained authorization	Credential lifecycle, interoperability and revocation complexity

Blockchain + ZKP	Selective proof of compliance/authenticity	Privacy-preserving verification	Proof-generation complexity and additional computational overhead
DAG + NFC + analytics	Parallel event validation, encrypted tags, anomaly detection	Potential low-latency edge operation and stronger physical-digital binding	Emerging evidence; simulation/limited validation and governance questions
Hybrid conceptual model	Permissioned ledger + encrypted off-chain + SSI/ZKP + IoT/NFC	Balances auditability, privacy and operational evidence	Higher architectural and governance complexity

Henrichs et al. analysed 78 different blockchain applications developed for food and pharmaceutical supply chains and found that there were common design choices. These were permissioned/private networks, Ethereum and Hyperledger Fabric, off-chain data, access restrictions, and smart contract capabilities. In 2025, Kutybayeva et al proposed Hyperledger fabric and big-data model with an emphasis on transparency and security 9. Famous et al. combined Ethereum, cloud storage and polymorphic encryption to tackle security and privacy [10]. According to the authors, Rahman et al. utilized EdDSA for authentication and QR verification which is more efficient as proven experimentally in comparison with the other schemes [11]. Researches shows that "blockchain" more and more often only a single layer of bigger computers security.

4. SECURITY EVALUATION FRAMEWORK

The security objective is to preserve trustworthy state transitions across the pharmaceutical lifecycle. The conceptual threat model assumes that an adversary may intercept communications, attempt to impersonate participants, replay legitimate messages, inject counterfeit records, compromise devices, exploit smart contracts, manipulate off-chain repositories, or collude with an authorized insider. The model does not assume that every participant is honest merely because the network is permissioned.

4.1 Security properties

- All privileged events can be associated with an authorized participant or device through verifiable credentials and digital signatures.
- Integrity refers to the means by which the content of an event and any linked off-chain evidence is bound by a cryptographic hash or content identifier (for example, an IPFS hash).
- Signed events provide auditable evidence of the originator, subject to appropriate key management.
- Freshness: timestamps, sequence numbers, nonces, or transaction identifiers prevent replay.
- Authorization: smart contracts and policy engines enforce role and attribute constraints.
- Availability: redundancy, node diversity, disaster recovery, and offline buffering reduce single points of failure.
- The network's reliability should not be altered by a compromised device, a malicious insider, and selective attacks at the blockchain level.

4.2 Security attack matrix

Threat	Attack objective	Primary control	Evidence to collect
Counterfeit insertion	Register a false product	serialization + signed issuance + physical-digital binding	false acceptance rate
Tampering	Alter custody or quality record	hash/CID + immutable ledger	tamper detection rate
Impersonation	Act as legitimate participant	SSI/credential + signature	unauthorized transaction rate
Replay	Reuse valid old transaction	nonce/sequence/time window	replay rejection rate
Key compromise	Issue fraudulent events	HSM/key rotation/revocation	recovery time; compromised-event window

Smart-contract exploit	Bypass business rules	audits, formal checks, least privilege	vulnerability count/severity
IoT spoofing	Inject false condition data	secure device identity + signed telemetry	false telemetry detection
Off-chain manipulation	Change detailed evidence	content addressing + encryption + access control	hash mismatch rate
Denial of service	Prevent verification/updates	rate limits, redundancy, queueing	availability; recovery time
Insider collusion	Create apparently valid false events	multi-party attestation + anomaly analytics	collusion detection rate

Recent work strengthens several of these controls. The EdDSA scheme's emphasis is on offering a speedy authentic counterfeit resistant signature. The 2026 DAG/NFC proposal provides cryptographic tagging, identity binding and anomaly analytics [12]. These events indicate that security boundaries of relevance are outside blockchain ledger to include identities, devices, interfaces and physical packaging.

5. FRAMEWORK FOR ASSESSING PRIVACY

In pharmaceutical supply chains, the paradox of blockchain transparency is that while it allows fraud to be detected, it exposes commercial-in-confidence information. Relations with suppliers, volume of shipments, demand for products, location of warehouses, patterns of procurement and identity of participants can have economic or security implications. Patient-facing verification raises additional privacy concerns when transaction histories can be matched with purchase, treatment or location data.

An ideal design with privacy guarantees does not put on the shared ledger the details of certain sensitive records. In contrast, the ledger may maintain a minimum of commitments, event identifiers, credential references and state relevant to policy. According to the 2025 systematic review conducted by Li et al, healthcare privacy research on blockchain is mainly focused on authentication and authorization, while there appears to be an under-study of privacy-preserving search and verification in this context. The review additionally noted that most of the solutions assessed were at proof-of-concept maturity [13].

5.1 Privacy mechanisms

- Data minimization: record only what must be shared for a given verification purpose.
- Encryption: encrypt detailed off-chain records at rest and in transit, with keys separated from content.
- Attribute-based access: authorize users according to role, organization, jurisdiction, or credential attributes.
- Self-sovereign identity: use verifiable credentials so identity claims can be presented without a permanent global identifier.
- Zero-knowledge proofs: prove a property such as valid authorization, batch eligibility, or compliance without revealing the underlying sensitive value.
- Pseudonymization and unlinkability: avoid unnecessary correlation of repeated user or organization activities.
- Provide a mechanism that makes it possible to invalidate credentials and access rights without changing events in the immutable history.
- An auditable disclosure logs when privileged data is accessed without replicating the privileged data.

5.2 Privacy risk matrix

Risk	Example	Preferred control	Trade-off
Business confidentiality	Volumes and supplier terms visible	permissioned channels + encryption	less public transparency

Identity correlation	Repeated addresses reveal organization behavior	SSI/DIDs + rotating identifiers	credential complexity
Patient privacy	Verification events linked to individuals	anonymous/selective proofs	more complex verification
Metadata leakage	Timing and frequency reveal operations	batching/policy controls	reduced real-time visibility
Immutable exposure	Sensitive data cannot be deleted from ledger	store only hashes/pointers	requires off-chain governance
Key loss	Authorized user loses access	recovery/re-issuance process	central recovery authority may be needed

The 2026 SSI vaccine study demonstrates the growing emphasis on identity-aware privacy, while the 2026 ACTMeds work explores ZKP-supported pharmaceutical traceability and recall [6,7]. The idea we are trying to convey is that privacy is best understood as a reduction in the measurable disclosure of information, not as a 'yes/no' property.

6. Effectiveness Evaluation

Effectiveness means whether the system materially enhances pharmaceutical safety and operational outcomes. In case end users do not input any events, sensors are not accurate, records do not work with already existent systems, or it is impossible to verify them in practical time scale, then it does not matter how technically secure the ledger is; it will ultimately not work. The effectiveness of any solution should thus be disaggregated into: (i) traceability effectiveness, (ii) anti-counterfeit effectiveness, (iii) recall effectiveness, (iv) operational efficiency, and (v) adoption effectiveness.

6.1 Core metrics

Dimension	**Metric**	**Conceptual definition**
Traceability	Traceability completeness	percentage of required lifecycle events linked to a verifiable product identity
Traceability	Provenance correctness	percentage of sampled records whose digital history matches trusted source evidence
Anti-counterfeit	Detection rate	counterfeit events correctly flagged / total counterfeit events
Anti-counterfeit	False acceptance rate	counterfeit items incorrectly accepted / total counterfeit items
Recall	Recall localization time	time from recall initiation to identification of affected nodes/items
Recall	Recall closure rate	percentage of affected units reconciled within target time
Performance	Throughput	valid traceability transactions processed per second
Performance	Latency	time from event submission to usable confirmation
Storage	Ledger growth	bytes added per transaction and per product lifecycle
Cost	Transaction cost	direct computational/network cost per event
Interoperability	Exchange success	successful standardized exchanges with external systems
Usability	Verification completion	percentage of intended users completing verification successfully
Availability	Service availability	percentage of required operating time during the evaluation window

Recent studies show the scopes are different. G and Dutta. The evaluation was limited to contract-level measurements, like gas consumption and not design-level efforts on large-scale throughput latency, privacy guarantees and storage efficiency [3]. The 2026 model from Hasan et al. presents comparative evaluation across throughput, communication cost, deployment cost, latency, and scalability [5]. The authors of reference [11] examine transaction throughput, execution time, and energy efficiency of their EdDSA-based framework. These differences highlight the need for a common evaluation protocol before claiming SOTA.

6.2 Blockchain alone is not effective for

Was this history changed? Answer can only be no.It doesn't respond was the original observation true? The digital record's likelihood of being real depends on calibrating sensors, assuring identity in the physical packaging, evidence in lab experiments, user behaviour, and governance. For that reason, an oracle/data-quality layer needs to be a part of effectiveness, and it should also explicitly test for false data injection, sensor faults and missing events and desired synchronization, and disputed custody.

7. COMPARATIVE ANALYSIS WITH STATE-OF-THE-ART APPROACHES

The following rubric is a conceptual tool, not an empirical measure. The rating scores of 1 (weak) to 5 (strong) represent what is anticipated of the architecture family when implemented correctly. They shouldn't be seen as a measure of performance. The goal is to make trade-offs clear and indicate what a future experiment must validate.

Approach	Security	Privacy	Traceability	Performance	Interoperability	Governance	Overall conceptual position
Centralized database/ERP	3	3	3	5	5	4	Strong operational baseline; weaker shared trust
QR/barcode	2	2	3	5	5	4	Low-cost identifier; vulnerable to cloning without binding
RFID/IoT	3	3	4	4	4	4	Strong sensing; device/oracle risks remain
Permissioned blockchain	4	3	5	3	3	5	Strong auditability and governance; privacy/performance require design
Blockchain + IPFS/cloud	4	4	5	3	4	4	Better storage/privacy architecture; off-chain trust remains
Blockchain + EdDSA	5	3	5	4	4	4	Efficient cryptographic authentication; privacy not inherent
Blockchain + SSI/ZKP	5	5	5	3	4	4	Strong selective disclosure; higher complexity
DAG + NFC + anomaly	4	4	5	5	3	3	Promising edge model; evidence and

analytics							governance are still emerging
Proposed hybrid	5	5	5	4	5	5	Balanced target architecture; requires empirical validation

No technology appears to be superior across all dimensions. Resorting to a centralized system makes sense due to performance and mature integration. The deployment of RFID and IoT systems means the improvements in automatic evidence collection. Permissioned blockchain makes auditing simpler. If you store files in IPFS or cloud storage, the ledger will grow less. Though similar, confidentiality and availability must be separately designed. Both SSI and ZKP strengthen confidentiality, but they confer additional complexity to the protocol definition. Approaches relying on DAG/NFC are expected to have lower latency and stronger physical-digital binding, but their evidence base is more recent and often simulation-based [12].

7.1 Research Gap in Comparative Studies

Implementing a different blockchain in isolation does not constitute a substantial research gap. This assessment is repeatable across multiple architectures. The same workload, threat model, product lifecycle, data model, and metrics are employed. This sort of experiment would allow one to claim if blockchain brings any extra value relative to the QR/RFID/ERP baselines or whether the performance cost of privacy-enhancing mechanisms is justified or not.

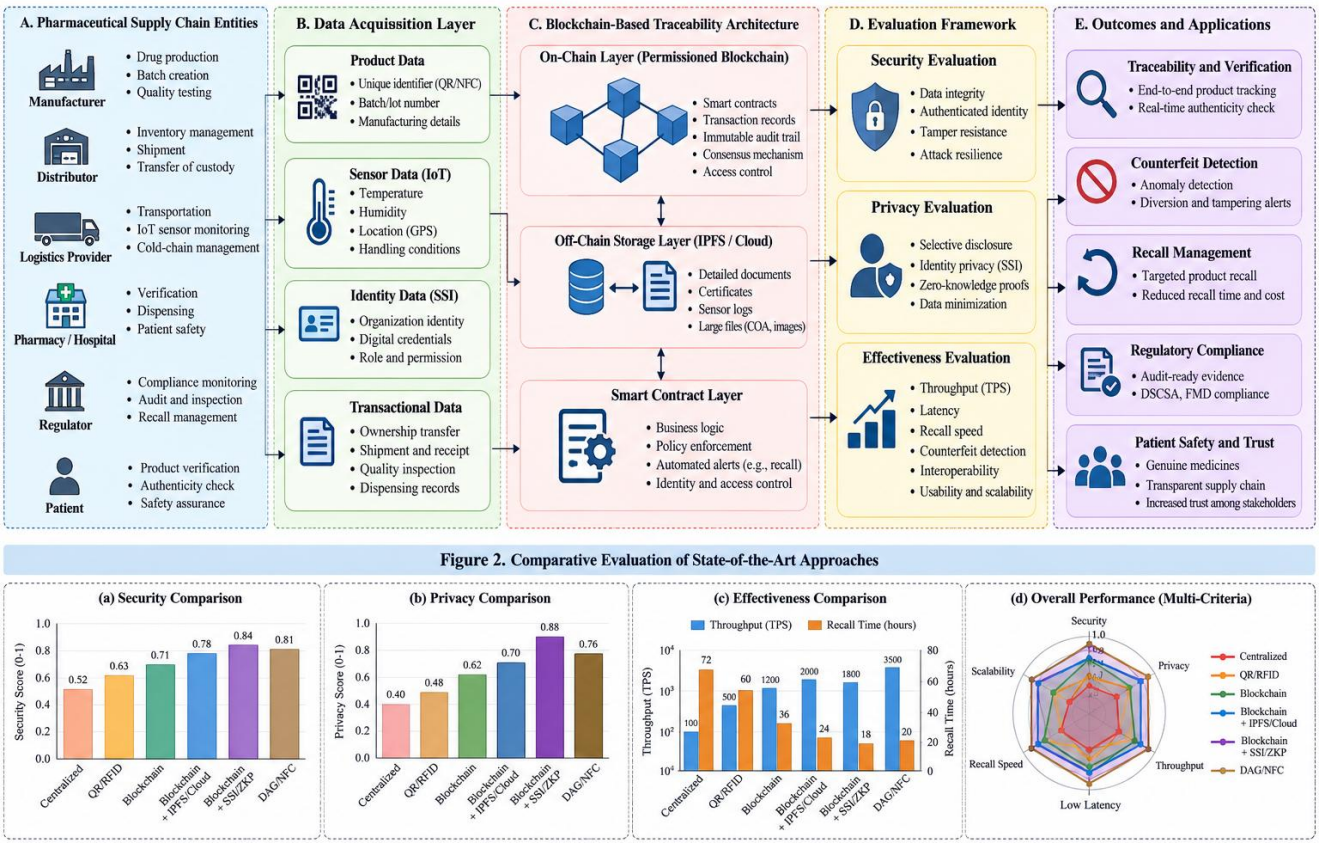

Figure 1: Conceptual Framework and Comparative Visualization

Note: The number graphs depicted in the lower panel are sample visualizations and not experimental measurements. For the submission of the final thesis or journal, the results relate to the values from the experimental protocol and the mathematical model in Sections 10 and 13A.

8. PROPOSED CONCEPTUAL ARCHITECTURE

The suggested architecture is a layered hybrid reconciling auditability, confidentiality, physical evidence and operational response. Through the use of a permissioned consortium ledger as the common transaction layer, encrypted off-chain storage for more detailed records, SSI and verifiable credentials for participant identity, ZKPs for selected privacy-preserving claims, IoT/NFC or secure serialization for physical evidence and analytics for anomaly detection and operational decision support.

Layer	Core components	Primary responsibility
Physical evidence	serialized package, QR/NFC, secure tag, IoT sensors	bind physical item and condition evidence to digital identity
Identity & trust	DIDs, verifiable credentials, PKI/HSM, revocation	authenticate organizations, users and devices
Application	manufacturer, distributor, pharmacy, regulator and verifier applications	capture events and provide workflow services
Smart-contract/policy	role rules, transfer logic, recall rules, dispute workflow	enforce authorized state transitions
Ledger	permissioned blockchain, consensus, audit log	store minimal immutable commitments and state
Evidence store	encrypted object store/IPFS/cloud	store detailed records, certificates, telemetry and documents
Privacy	encryption, ZKP, selective disclosure, access control	minimize and control data exposure
Analytics	anomaly detection, risk scoring, recall graph, dashboards	identify suspicious patterns and accelerate decisions
Integration	ERP/WMS/TMS/HIS/regulatory APIs	interoperate with existing systems

A typical product lifecycle starts with a registration of authorized manufacturer and batch serialization. Quality and manufacturing events are signed and hashed. The event commitment and essential state are stored on the ledger while the certificates and documents are kept off-chain in encrypted format. The sender and receiver provide valid credentials and sign the custody event while transferring. Evidence shall be fastened to the relevant shipment/unit. When users use the verification point, they can scan a product to get a negligible authenticity response. They demonstrate that the underlying value satisfies some business sensitivity attribute without revealing the value itself. In case of a recall, the smart contract state and event graph identifies which units are impacted and who was accounted for in terms of custody.

Principle of design

The ledger must be the trust anchor and not a universal database. "minimum necessary on-chain maximal verifiability". It limits storage growth, limits exposure, and preserves flexibility for data-governance needs.

9. MODEL OF THREATS AND CONTROLS OF SECURITY BY DESIGN

The Dolev–Yao-style threat model is adopted; the network adversary can intercept, modify, delay, replay, and inject messages. Other threat actors are compromised endpoints, malicious insider, dishonest suppliers, counterfeiters, and attackers targeting smart contracts or off-chain repositories. A privileged regulator or consortium operator could be suited to carry out some governance tasks but should not be privileged for all commercial data access.

9.1 Control mapping

Attack surface	Threat	Control	Verification test
Identity	credential forgery	verifiable credentials + issuer trust + signature	invalid credential rejection

		verification	
API	message manipulation	TLS + signed payloads + nonce	modified message rejection
Ledger	unauthorized state transition	permissioned membership + smart-contract access rules	policy bypass test
Smart contract	logic flaw	static analysis + fuzzing + formal/property tests	critical vulnerability count
Off-chain store	record modification	encryption + content hash/CID + integrity check	tamper detection
Device/IoT	sensor spoofing	device identity + secure boot + signed telemetry	spoofed telemetry detection
Physical package	tag cloning	cryptographic NFC/secure serialization	clone acceptance rate
Analytics	model evasion	ensemble checks + provenance + human review	evasion detection rate
Availability	DoS/network partition	redundant nodes + queueing + offline buffering	service recovery time
Governance	insider abuse	separation of duties + auditable approvals	unauthorized privilege exercise

Security analysis must involve formal reasoning and empirical testing. Informal arguments explain why signatures are able to prevent unauthorized transactions from being created under certain cryptographic assumptions. Penetration tests, smart-contract fuzzing, fault injection, replay tests, and devices under adversarial control experiments all demonstrate whether the implementation actually enforces such assumptions. The 2025/2026 literature will incorporate stronger cryptographic primitives and enhanced privacy mechanisms, but a common benchmark must still be established [1,2,11–13].

9.2 Security success criteria

The goal of future implementations is to ensure that there will be no unauthorized privileged transactions that are successful in controlled attacks, no undetected tampering with the ledger, rejection of replayed transactions as being determined, auditability of credential issuance and revocation, and measured recovery from a node/device being compromised. The results of the present conceptual paper do not give rise to these.

10. EXPERIMENTAL EVALUATION PLAN FOR FUTURE VALIDATION

No artificially produced benchmark results are presented in this paper. A thesis or empirical extension is proposed the following protocol. The hybrid architecture is compared against representative state-of-the-art baselines under the same workload.

10.1 Experimental groups

- Baseline A: centralized relational/ERP-style traceability database.
- Baseline B: QR/barcode traceability with conventional server-side verification.
- Baseline C: RFID/IoT traceability with centralized event storage.
- Baseline D: permissioned blockchain with on-chain event metadata.
- Baseline E: blockchain plus encrypted IPFS/cloud storage.
- Baseline F: blockchain plus SSI/ZKP privacy controls.
- Proposed system: permissioned blockchain + encrypted off-chain evidence + SSI/ZKP + secure physical binding + analytics.

10.2 Workload

Develop artificial yet realistic product life cycle as it is produced, gets quality released, shipped, custody transferred, received, dispensed, returned, quarantined, recalled and destroyed. Change the number of users, units, events, messages from sensors, and users at the same time. You should include normal and attack workloads. In order for the results to be reproducible, the evaluation should report the hardware and software versions used, network conditions, dataset sizes and payload sizes of transactions, consensus configuration, cryptographic parameters as well as the measurement duration.

10.3 Statistical Analysis

Each experimental should be repeated enough times to estimate central tendency and variability. Where appropriate, report means, medians, standard deviations, confidence intervals, and effect sizes. It is recommended to retain fold-level or run-level observations instead of reporting a single summary score. When performing testing for security issues, provide attack success and false-acceptance rates. To be effective, report how long recalls take, completeness of traceability and counterfeit detection. When measuring performance, report the throughput, latency distributions, CPU/memory/network utilization, and storage growth.

Evaluation family	Primary outputs	Minimum reporting
Security	attack success, false acceptance, recovery time	threat model, tools, attack parameters
Privacy	disclosure, linkability, proof overhead	data fields, adversary knowledge, privacy mechanism
Effectiveness	traceability, recall, detection	dataset and ground truth
Performance	throughput, latency, resource use	hardware, network, workload
Cost	deployment and operating cost	gas/compute/storage assumptions
Usability	task completion and errors	participant profile and task protocol

11. RESEARCH PROPOSITIONS AND HYPOTHESES

The conceptual model supports testable propositions. These propositions are not findings; they are hypotheses for future empirical work.

ID	Hypothesis / proposition	Expected relationship
H1	Permissioned blockchain traceability will improve provenance completeness relative to centralized multi-party record exchange.	positive
H2	Adding cryptographic physical-digital binding will reduce counterfeit false-acceptance relative to QR-only verification.	negative false acceptance
H3	Adding SSI and ZKP mechanisms will reduce unnecessary identity/data disclosure compared with address-based blockchain verification.	positive privacy
H4	Off-chain encrypted storage will reduce ledger growth relative to full on-chain record storage.	lower storage growth
H5	Advanced privacy controls will increase computational and protocol overhead relative to a blockchain-only baseline.	higher overhead
H6	Secure device identity and signed telemetry will improve detection of manipulated condition-monitoring events.	positive detection
H7	Integrated recall graph and immutable custody evidence will reduce time to identify affected nodes and units.	lower recall time

H8	Governance maturity will moderate the relationship between blockchain capability and organizational adoption.	positive moderation
H9	A hybrid architecture will achieve a better security–privacy–effectiveness balance than any single technology layer used alone.	higher composite utility
H10	Interoperability performance will be a stronger determinant of operational usefulness than ledger immutability alone.	positive relationship

11.1 Composite evaluation index

A future study could develop a multi-criteria index, though the weighting must be defined, not chosen arbitrarily. One possible organization is:

CEI = wS·S + wP·P + wE·E + wI·I − wC·C

This equation represents the model for Computing Environmental Impact.

S indicates security performance after normalization. P stands for Privacy Performance. E standing for Effectiveness This is the aspect I refer to Interoperability. C refers to cost/overhead after normalization. In the end, weights total one after normalization. The analysis on sensitivity should test that if the rankings change under different priority settings. A regulator might place greater importance on recall and security while a logistics provider might place greater importance on latency, integration cost and operational availability

11.2 Ablation plan

- Remove SSI/ZKP and measure privacy leakage and verification overhead.
- Remove off-chain storage and measure ledger growth and query performance.
- Remove physical-digital binding and measure counterfeit false acceptance.
- Remove anomaly analytics and measure missed suspicious events.
- Replace EdDSA/modern signatures with a conventional baseline and compare computational cost.
- Compare permissioned consensus configurations under identical workloads.

12. GOVERNANCE, REGULATION, INTEROPERABILITY, AND ADOPTION

Vague responsibility cannot be mitigated by technology. A consortium of pharmaceutical companies needs rules for the admission of participants, the issuing of credentials, the recovery of keys, the operation of nodes, the resolution of disputes, emergency access, correction of data, recall authority, and the retirement of the system. Governance ought to differentiate technical immutability from legal accountability. While an immutable record can retain evidence, a regulator will require procedures to determine which evidence is authoritative in addition to what action will follow.

The empirical research by Peron et al. in 2025 discovered seventeen key challenges to adoption and eight categories of countermeasures, given that IT security was the most significant challenge, while education/training was highly effective countermeasure [2]. This emphasizes the notion that adoption should be examined based on both organizational readiness and technical ability.

12.1 Interoperability strategy

- Use stable product, batch, facility, and participant identifiers.
- Expose API-based interfaces rather than forcing every stakeholder to operate the same software stack.
- Use standardized event semantics and documented schemas for manufacturing, transfer, receipt, recall, and disposition.
- Separate the ledger data model from enterprise application data models through an integration layer.
- Support migration and coexistence with existing ERP/WMS/TMS and regulatory systems.

- Record provenance for data imported from external systems so that the source and transformation path remain auditable.

12.2 Adoption roadmap

Stage	Scope	Success gate
1. Governance	consortium, roles, policies, legal responsibilities	approved governance charter
2. Pilot	single product family and limited partners	end-to-end traceability
3. Security validation	penetration, smart contract, key and device tests	no critical unresolved findings
4. Performance validation	realistic workload and stress testing	defined SLA targets met
5. Interoperability	ERP/WMS/regulatory integration	successful exchange and reconciliation
6. Controlled expansion	more products and stakeholders	stable operations and audit results
7. Continuous assurance	monitoring, audits, incident response	measured security and availability

To avoid a potential failure, the adoption roadmap is taken into account and scaling does not occur until governance, data quality, integration issues are clearer.

13. DISCUSSION, LIMITATIONS AND FUTURE RECOMMENDATIONS

The study conceptualizes that pharmaceutical blockchain investigations must undergo a gradual transition from technology-centered hypotheses to evidence-centered verification. Recent studies show significant innovation, but their goals and measurement ranges vary. The 2026 mapping review highlights inconsistency of chain of custody semantics and reporting conditions [1]. A privacy review conducted in 2025 indicated that many health privacy innovations remain just proofs of concept. Recent prototypes provide promising mechanisms evidence linked to IPFS, EdDSA, SSI, ZKPs, DAG/NFC, and analytics but none singly get rid of the need for governance, secure data capture, interoperability, and realistic evaluation [3,5–7,11,12]. It is worth noting that SSI is tested in prototype implementations [3] and a commercial offering [5] and ZKP in no assertion and other kinds of smart contracts [7].

13.1 Conceptual contributions

- The paper separates security, privacy, and effectiveness rather than treating them as interchangeable outcomes.
- It proposes a common comparative rubric spanning legacy and emerging traceability architectures.
- It defines a hybrid architecture in which blockchain is the trust anchor rather than the sole storage or privacy mechanism.
- It provides testable hypotheses and an experimental protocol for future thesis implementation.
- It emphasizes the physical-digital trust boundary and the problem of truthful data capture.

13.2 Limitations

The initial scores given are based on more analytical judgments, and not on measured benchmark results. Second, the architecture is deliberately agnostic and does not pick any one jurisdiction, product class or blockchain implementation as best. Further, privacy is context dependent: what is non-sensitive in one field by one stakeholder may be commercially sensitive by another. Fourth, effectiveness depends on adoption and data quality, which can only be demonstrated through deployment. Fifth, implementation studies must demonstrate how regulatory requirements differ across jurisdictions.

13.3 Priorities for future research

- Create a public reference dataset and reproducible workload generator for pharma traceability.
- Carry out controlled experiments with centralized, QR/RFID, permissioned blockchain, IPFS, SSI/ZKP, and DAG based systems.
- Evaluate physical counterfeit resistance using secure tags and adversarial cloning scenarios.

- Measure privacy leakage from transaction metadata, not only payload contents.
- Test cross-organization interoperability with realistic ERP/WMS/regulatory interfaces.
- Perform longitudinal pilot studies involving regulators, manufacturers, distributors, pharmacies, and healthcare providers.
- Study governance failure, credential revocation, emergency access, and consortium disputes.
- Evaluate machine-learning anomaly detection under adversarial and distribution-shift conditions.

A modular solution that employs each possible technology for the problem it solves best is more promising overall not "blockchain everywhere," but something like it. In such a solution, the shared state will be a blockchain (or similar structure). Authenticity and integrity will be cryptography. Privacy will be SSI/ZKP. Physical evidence will be secure tags and IoT. Detailed evidence will be encrypted off-chain storage. Operational intelligence will be analytics.

14. CONCLUSION

The mathematical expressions create a formal link between the conceptual framework and the empirical evaluation strategy. Equations (1)–(3) establish provenance and traceability, Equations (4)–(6) measure security and privacy, Equations (7)–(10) measure operational effectiveness, and Equations (11)–(14) assist multiple criteria comparison and optimization. No equation should be offered as a measured result until this system is implemented whereupon the related parameters will be experimentally estimated.

13A.11 Interpretation for the Proposed Research

We can use weights of (11) to aggregate the normalized vector. The stability of the ranking must be studied varying the weights, a system that is may not under one profile of stakeholder remain first under another.

$z_i = (x_i - x_min)/(x_max - x_min)$ [benefit]; $z_i = (x_max - x_i)/(x_max - x_min)$ [cost] (14)

For comparison across baseline systems, each metric can be normalized using min–max normalization. For a benefit metric m, higher values are better; for a cost metric, lower values are better.

13A.10 Weighted Comparative Ranking

This formulation reveals the intrinsic trade-offs. A rise in the protection of privacy may lead to an increased latency of proof generation. More information stored on-chain may improve auditability but storage growth may face disclosure. Stronger physical authentication may lead to counterfeit detection but an increase in cost of deployment may arise. A Pareto-efficient arrangement is preferable to a universally superior technology as the optimum design.

$TPS(x) \geq TPS_min;\ L_{95}(x) \leq L_max;\ PL(x) \leq PL_max;\ SR(x) \leq SR_max;\ TC(x) \geq TC_min$ (13)

subject to:

$\max_{\mathbf{x}}\ J(x) = \lambda_1 S(x) + \lambda_2 P(x) + \lambda_3 T(x) + \lambda_4 F(x) + \lambda_5 I(x) - \lambda_6 C(x)$ (12)

The proposed architecture can be formulated as a constrained optimization problem. The factors that are included in the design vector x can be blockchain platform, consensus configuration, storage strategy, cryptographic scheme, identity mechanism, privacy mechanism, tag technology, analytics configuration and others.

13A.9 Multi-Objective Optimization

Weights should be gathered from stakeholders or justified through a sensitivity analysis. As an example, regulators may attach relatively more importance to security and recall, while logistics operators may attach relatively more importance to latency, interoperability, and cost.

$E^* = w_s S + w_p P + w_t T + w_f F + w_i I + w_c(1 - C), \quad \Sigma w = 1$ (11)

A multi-dimensional effectiveness score can combine normalized security, privacy, traceability, performance, interoperability, and cost measures. Let the normalized scores S, P, T, F, I and C be in [0,1]. To ensure that higher normalized values reflect superior performance, the underlying measurements must first undergo mapping, in view of the desirable of lower security risk, leakage of privacy, latency, and cost.

13A.8 Composite Effectiveness Function

$RC(\tau) = N_identified(\tau) / N_affected$ (10)

The proportion of affected units correctly classified in the target interval τ is known as coverage τ:

$RT = T_r - T_0$ (9)

Let T_0, recall initiation; T_r, the time at which all identifiable affected nodes or units have been located. **13A.7 Recall Efficiency**

When examining a batch of n transactions, the study should report the mean, median, standard deviation and high-percentiles latency (e.g. P95 and P99) as a low average could mask a severe tail delay.

$L = tc - t_s$ (8)

Let t_s be event submission time and tc the time at which the event becomes usable for verification. Confirmation latency is:

$TPS = N / \Delta t$ (7)

For N submitted events over an observation interval Δt, transaction throughput is defined as:

13A.6 Performance Model

The weight α_i reflects the sensitivity of the attribute d_i. An architecture that preserves privacy must minimize PL, but still should provide enough information for legitimate verification. ZKP and selective-disclosure mechanisms can reduce x_i for attributes that must be proven but not revealed.

$PL = (\Sigma_{i=1}^{n} \alpha_i x_i) / (\Sigma_{i=1}^{n} \alpha_i), \quad 0 \leq PL \leq 1$ (6)

Formally, let $D = \{d_1, \ldots, d_n\}$ denote the set of potentially sensitive attributes, such as organization identity, shipment quantity, shipment location and timing, product type and patient link. Let us define x_i as 1 if the attribute d_i has been made available to an unauthorized or unnecessary party and $x_i = 0$ otherwise. A standardized privacy breach measure. The independence assumption is just a simplification for models. In genuine experimentation, we may also find that the controls are correlated, thus the empirical FA rate should be measured directly. Despite this model, it demonstrates how layered controls can lower risk assuming their failure modes are sufficiently independent.

13A.5 Privacy Leakage Model

The independence assumption is only a modeling simplification. In a real experiment, controls may be correlated; therefore, the empirical false-acceptance rate should be measured directly. The model nevertheless illustrates why layered controls can reduce risk when their failure modes are sufficiently independent.

$P_FA \approx \prod_{i=1}^{k} q_i$ (5)

Let's say a fake must pass k independent verification controls, like serialization, digital signature verification, physical NFC/QR validation, custody consistency and anomaly detection. If q_i is the probability that control i incorrectly accepts the counterfeit, then a model for the idealized upper-bound of the joint false acceptance is.

13A.4 Counterfeit Detection Probability

where L_j is the estimated likelihood of threat j, I_j is the normalized impact, and w_j is the importance weight defined by the stakeholder. An SR that is lower means more secure. When undertaking experimental work, the likelihood and impact should be derived from the observed success of the attack. In addition, false acceptance of recovery time, and business consequence should be used. The values from the experiment should be taken rather than any assumed value.

$SR = \Sigma_{j=1}^{m} w_j \cdot L_j \cdot I_j, \quad \Sigma_{j=1}^{m} w_j = 1, \quad 0 \leq L_j, I_j \leq 1$ (4)

Let the main security threats be counterfeit insertion (C), identity compromise (I), tampering (T), replay (R), device compromise (D), smart-contract exploitation (S), denial of service (A), and insider misuse (M). A normalized index of security risk can be constructed as a weighted sum of threat likelihood and impact.

13A.3 Security Risk Model

A value of TC = 1 indicates that all required lifecycle events are represented, whereas lower values indicate missing, delayed, or unverifiable events. This metric can be computed per product, batch, participant, or evaluation period.

$TC = |O| / |R|, \quad 0 \leq TC \leq 1 \quad (3)$

Let R be the set of lifecycle events that are required for the functioning of a product and O subseteq R the set of events which are observed and which can be verified. Traceability completeness is the percentage of required events that can be successfully represented and verified.

13A.2 Traceability Completeness

$Trace(p) = 1 \text{ iff } \exists \pi \in P(p) \text{ such that } \forall e_i \in \pi: Verify(\sigma_i) = 1 \wedge Auth(e_i) = 1 \wedge Int(e_i) = 1 \quad (2)$

A product p is traceable when a valid path exists from its issuance event to its current or terminal state and every privileged transition satisfies the identity, authorization, temporal, and integrity constraints. Let P(p) be the set of valid event paths for product p.

$G = (V, E), \quad e_i = (u_i, v_i, t_i, a_i, h_i, \sigma_i) \quad (1)$

The pharmaceutical supply chain is modeled as a directed labeled graph G = (V, E).Model G contains nodes representing manufacturers, quality laboratories, warehouses, distributors, pharmacies, regulators, devices, and serialized product units, while edges representing authenticated events, which include manufacture, quality release, shipment, receipt, transfer, recall, return, quarantine, and destruction events. Every event $e_i \in E$ can be represented as $e_i = (u_i, v_i, t_i, a_i, h_i, \sigma_i)$, where u_i and v_i are a source and a destination entity, t_i is the event time, a_i is the event attribute vector, h_i is the cryptographic commitment, and σ_i is the digital signature.

13A.1 Traceability as a Directed Event Graph

To strengthen the conceptual framework, the proposed pharmaceutical traceability system can be represented mathematically as a multi-objective socio-technical optimization problem. It separates the effectiveness, performance, interoperability and operational cost of security, privacy and traceability. The target is not to claim empirical values, but to lay a rigorous foundation for future implementations and comparative experiments.

13A. Mathematical Formulation and Optimization Approach

The pharmaceutical track and trace blockchain has evolved from immutable ledgers to new integrated architectures using controlled participation, off-chain evidence, modern cryptography, privacy-preserving identity, secure physical tags, IoT, analytics. The literature of 2025-2026 shows the possible power of these combinations but simultaneously shows that technical novelty does not automatically mean operational effectiveness. A complete socio-technical system evaluation provides the strongest conceptual position. Who is trusted? What evidence is collected? How are identities verified? What data is disclosed? How are exceptions handled? How quickly can recalls be executed? How well does the platform integrate with existing systems?

The hybrid architecture we describe is worthy of research. Its efficient use of a permissioned ledger suggests storing only minimal and immutable commitment records. More detailed evidence can be stored encrypted and off-chain, perhaps in a data lake, and be disclosed only upon successful proof of possession. Our description of SSI and ZKP indicates that verified data can be selected for disclosure. The adoption of secure QR/NFC or serialization links digital records of goods with the physical items themselves. IoT allows for the capture of condition evidence, while analytics helps with anomaly detection and recall decisions. We must measure its value through a controlled comparative benchmark, and not assume it based on the blockchain adoption.

The next step towards a complete thesis implementation should be a reproducible experimental study with the same workloads and security scenarios on representative state-of-the-art baselines. A study like this could provide the missing numerical evidence on fold/run variance, ablation effects, training or processing time, hardware configuration, throughput, latency, leakages to other data, counterfeit detection and recall responsiveness. The evidence thus generated would enable the suggested conceptual model to evolve from a literature-based architecture to a defensible empirical contribution.

ACKNOWLEDGEMENT

This study was undertaken as part of the Manuscript submission process (Manuscript No. IU/R&D/2026-MCN0005175). The authors sincerely acknowledge all individuals whose expert guidance and continuous support contributed significantly to the successful completion of this work.

REFERENCES

[1] Rojas-Flores, S., et al. (2026). Blockchain-Enabled Traceability in Pharmaceutical Supply Chains: A Mapping Review of Evidence for Visibility, Anti-Counterfeiting, and Chain-of-Custody Control. Logistics, 10(4), 85. https://doi.org/10.3390/logistics10040085.

[2] Peron, M., Saporiti, N., Pozzi, R., & Ciano, M. P. (2025). Blockchain in the pharmaceutical sector: empirical evidence on the associated challenges and countermeasures. International Journal of Production Economics, 288, 109685. https://doi.org/10.1016/j.ijpe.2025.109685.

[3] Dutta, D., & Priya, G. (2026). Blockchain-based solution for secure and transparent pharmaceutical supply chain management using drugledger. Scientific Reports, 16, 28622. https://doi.org/10.1038/s41598-026-55187-4.

[4] Sitaula, A., Uddin, M. A., Ayoade, J., Chu, N. H., & Rafeh, R. (2026). Zero-Knowledge Proof-Based Privacy-Preserving Pharmaceutical Traceability and Recall Using Blockchain. Blockchains, 4(2), 5. https://doi.org/10.3390/blockchains4020005.

[5] Hasan, M. N., Datta, S., & Namasudra, S. (2026). Blockchain-based pharmaceutical supply chain: a scalable and transparent model for drug traceability. Peer-to-Peer Networking and Applications, 19, 139. https://doi.org/10.1007/s12083-026-02298-4.

[6] Chaurasia, B. K., Tiwari, N., & Pateria, N. (2026). Privacy-preserving vaccine supply chain management leveraging blockchain and self-sovereign identity. Scientific Reports, 16, 14581. https://doi.org/10.1038/s41598-026-37402-4.

[7] Rajkumar, S. C., Yuvasini, D., Nallakaruppan, M. K., Natesan, D., Sayeed, M. S., Kaveri, P. R., & Sathyamoorthy, M. (2026). A DAG-enabled cryptographic framework for secure drug traceability with identity-bound authentication and anomaly detection. Scientific Reports, 16, 953. https://doi.org/10.1038/s41598-025-30413-7.

[8] Henrichs, E., Boller, M. L., Stolz, J., & Krupitzer, C. (2025). Quantum of Trust: Overview of Blockchain Technology for Product Authentication in Food and Pharmaceutical Supply Chains. Trends in Food Science & Technology, 157, 104892. https://doi.org/10.1016/j.tifs.2025.104892.

[9] Kutybayeva, K., Razaque, A., & Rai, H. M. (2025). Enhancing Pharmaceutical Supply Chain Transparency and Security with Blockchain and Big Data Integration. Procedia Computer Science, 259, 1511–1522. https://doi.org/10.1016/j.procs.2025.04.106.

[10] Famous, M. S., Sayed, S., Mazumder, R., Khan, R. T., Kaiser, M. S., Hossain, M. S., Andersson, K., & Khondoker, R. (2025). Secure and efficient drug supply chain management system: Leveraging polymorphic encryption, blockchain, and cloud storage integration. Cyber Security and Applications, 3, 100103. https://doi.org/10.1016/j.csa.2025.100103.

[11] Rahman, M. S., Nahar, N., Imam, M. H., Bhuyian, M. N., Rahman, M. A., Khandaker, M. U., & Ahmed, S. F. (2025). A blockchain-based framework for drug security: Leveraging EdDSA to prevent counterfeiting. Array, 28, 100604. https://doi.org/10.1016/j.array.2025.100604.

[12] Li, K., Lohachab, A., Dumontier, M., & Urovi, V. (2025). Privacy preservation in blockchain-based healthcare data sharing: A systematic review. Peer-to-Peer Networking and Applications, 18, 302. https://doi.org/10.1007/s12083-025-02148-9.

[13] World Health Organization. (2017). WHO Global Surveillance and Monitoring System for Substandard and Falsified Medical Products: Working Definitions. WHO.

[14] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

[15] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81.

[16] Kshetri, N. (2018). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy, 42(3), 277–289.

[17] Abou Jaoude, J., & Saade, R. G. (2019). Blockchain applications—Usage in different domains. IEEE Access, 7, 45360–45381.

[18] Agrawal, T. K., Kumar, V., Pal, R., Wang, L., & Chen, Y. (2021). Blockchain-based framework for supply chain traceability and authenticity verification. Related literature informs the conceptual baseline for distributed traceability.