

Optimising the Drug Supply Chain Using Blockchain

Siddesh Jayaraman¹

Received February 16, 2026

Accepted July 31, 2026

Electronic access October 31, 2026

Falsified medicines kill patients who believe they are being treated. In low- and middle-income countries, the World Health Organization puts the share of substandard or falsified medical products at about one in ten. An antibiotic with too little active ingredient doesn't clear the infection that it was prescribed for. Track-and-trace still depends on paper forms and company databases that aren't able to read one another. A fake batch can move through several wholesalers and distributors before anyone checks which of them held it. Researchers have proposed blockchain ledgers to close this gap. Most of those designs have only run in small pilots, and few explain how they would protect commercial data or connect to existing company systems. Much of the published cost discussion relies on public-blockchain gas fees that permissioned networks never charge. This study designs a four-layer blockchain and Internet of Things (IoT) architecture for pharmaceutical traceability and tests it against what published permissioned systems achieve. No physical prototype was implemented. The study specifies the architecture and walks its smart-contract logic through representative supply-chain scenarios, then maps each WHO and FDA traceability requirement onto the design feature that addresses it. Every performance expectation comes from published benchmarks rather than measurement. In the walkthroughs, the contract logic behaves as specified, and every requirement examined maps onto a design feature. Commercially sensitive information stays off the shared record in off-chain storage. The study produces a specification and a cost model built for permissioned networks, and a pilot deployment could test both.

Keywords: blockchain; Internet of Things; pharmaceutical supply chain; drug traceability; smart contracts; permissioned ledger; conceptual framework .

Introduction

Background and Context

Patients usually cannot tell a counterfeit or adulterated medicine from a genuine one, and such products still reach them through the pharmaceutical supply chain. According to World Health Organization (WHO) estimates, roughly one in ten medical products circulating in low- and middle-income nations is substandard or falsified^{1,2}. These substandard and falsified medical products (SFMP) can carry the wrong dose of the active ingredient, or none of it. Patients who receive them fail to improve, and some die of conditions the genuine drug would have treated¹. Each time fakes are found in legitimate channels, patients become more wary of the real medicines stocked beside them, vaccines included. Even the tightly regulated UK market has been affected. In 2005, counterfeit Lipitor printed with a genuine batch number reached British pharmacies, and 120,000 packs were recalled. Fakes from the same batch were still turning up in 2006^{3,4}.

Existing traceability systems often miss these products. Custody transfers in many supply chains are still logged on paper or in a single company's database, and one company's

records rarely link to the next⁵. A wholesaler receiving a batch therefore cannot query the manufacturer's record of that batch directly. This disconnection lengthens recall response times and makes the route of a suspect batch difficult to reconstruct⁶. The organisation that owns a centralised repository can also alter historical records after the fact. Independent copies do not exist elsewhere, and a single compromised system destroys the entire custody history⁷.

The Role of Blockchain and IoT in Supply Chain Visibility

Supply chain research treats end-to-end visibility as the condition that lets partners catch a bad batch quickly and establish who handled it⁸. A blockchain provides it with an append-only ledger, copied in full to every participant. A shipment entry cannot be altered once written, and no single company controls the stored history⁹. A conventional shared database offers no equivalent guarantee against later alteration. A permissioned network restricts participation to vetted organisations while keeping the shared state consistent among them⁷. Code attached to the ledger, known as a smart contract, checks each custody transfer against the applicable business rules before the transfer is recorded. Manual verification at each hand-off is no longer required¹⁰.

¹ Oaks Christian School, Thousand Oaks, California, USA

IoT devices link each physical product to its ledger record. At each checkpoint, a reader scans the product's RFID tag or near-field communication (NFC) label and records the scan on the ledger. Environmental sensors write temperature and humidity readings during transit¹¹. Lightweight RFID authentication schemes can also detect cloned or replayed tags at transfer points¹².

The MediLedger pilot put part of this architecture into production, with a permissioned blockchain carrying interoperable traceability data from manufacturers to dispensers under U.S. Drug Supply Chain Security Act (DSCSA) requirements^{13,14}.

Persisting Challenges

Successful pilots have not produced wide adoption. Transaction flows on a shared ledger reveal which organisations trade with which and in what volume, and firms treat that information as commercially sensitive¹⁰. Scalability is a recognised constraint on blockchain adoption in supply chain operations¹⁵. Interoperability remains limited by incompatible data standards across legacy enterprise systems¹⁴. Most proposed frameworks have been tested only in small pilots or simulations, and there is little record of how they behave in a live supply chain¹⁶. Of the four barriers, this lack of real-world evidence is the most serious.

Research Questions and Objectives

Three questions guide this study:

1. Can a four-layer permissioned blockchain and IoT architecture be specified in enough detail to trace products end to end, and to block unauthorised transfers, across a multi-stakeholder pharmaceutical supply chain?
2. When the proposed smart-contract logic is walked through representative supply-chain scenarios, does it enforce the intended handoff and identity rules and flag storage-condition violations?
3. How closely does the design align with WHO and FDA traceability requirements, and what do published benchmarks of comparable permissioned systems suggest about its performance and cost?

The first objective is to design a permissioned consortium blockchain architecture with IoT integration and smart-contract enforcement. The second is to specify the contract logic and evaluate it by walkthrough against representative supply chain scenarios. The third is to map the design against compliance standards and to draw expected performance and cost ranges from published prototypes of comparable systems.

Contributions of This Study

The study makes four contributions:

- A four-layer permissioned blockchain and IoT framework whose specification covers the data flows between layers and the role-based smart-contract logic governing each transfer, with sensitive commercial attributes held off-chain.
- A comparative synthesis of prior frameworks (Table 1), paired with a cost model built for permissioned infrastructure. Much of the cost discussion in the literature is framed in public-blockchain gas fees that permissioned networks do not charge. This study builds its cost model from infrastructure and operations instead.
- A direct mapping between design features and regulatory obligations, covering WHO cold-chain guidance and FDA DSCSA traceability requirements.
- A clear boundary between what was designed and what was demonstrated. The architecture is a specification rather than a tested system, and no performance figure in this paper is a measurement of it.

Literature Review

Blockchain and IoT for Pharmaceutical Traceability

Counterfeit circulation and opaque provenance have pushed researchers toward blockchain as a traceability tool. Once a manufacturing or handoff event is written to an append-only shared ledger it cannot be removed, and every authorised party reads the same history from production through to dispensing^{9,17}. Early studies identified a lower incidence of SFMP and faster recalls as the two main benefits. The same studies were equally clear about the technical and organisational difficulty of implementation⁹. Later reviews have catalogued the architectures proposed for drug traceability along with the challenges that remain open¹⁸.

IoT hardware supplies the link between a physical drug unit and its ledger record. RFID tags and NFC labels identify the unit. Environmental sensors record the temperature and humidity around it, and every scan and reading carries a location and a time^{19,20}. A gateway, or middleware, layer connects the devices to the ledger. It packages each incoming reading as a structured transaction and submits it to the blockchain network, where smart contracts validate the transaction before it is committed^{11,19}. Figure 1 illustrates this flow, in which a chain of custody is verified by machines rather than assembled from manual records.

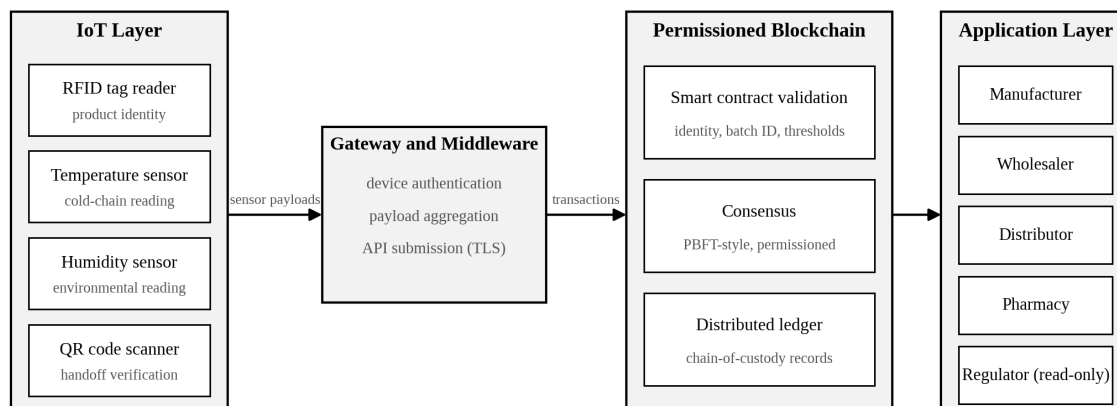


Figure. 1 Blockchain and IoT interaction in the pharmaceutical supply chain. All write operations pass through smart-contract validation before being committed as an immutable, timestamped ledger entry. Sensitive business attributes are stored off-chain, with only cryptographic hashes anchored on the ledger.

Proposed Systems and Comparative Assessment

Many frameworks and prototype systems have been proposed for blockchain-enabled pharmaceutical supply chains. Table 1 compares the prominent ones across platform, privacy features, reported throughput, and noted limitations.

Across these proposals, permissioned networks recur as the platform of choice²¹. Hyperledger Fabric is the most common selection. It restricts participation to authorised entities and supports complex chaincode, the platform’s term for smart contracts. Its channels, private sub-ledgers visible only to the organisations admitted to them, also suit an industry that guards commercial data closely²¹. Public blockchains such as Bitcoin or Ethereum charge a cryptocurrency transaction fee on every write. Permissioned ledgers charge none, and that distinction governs the cost modelling in Section “Cost Considerations under a Permissioned Architecture”.

Smart contracts are the other defining feature of these designs. Several authors describe per-shipment validation logic that verifies authenticity at each handoff and flags discrepancies^{10,19}. The contracts also carry role-based access control. Only authorised actors can update or query particular ledger data. In Singh et al.’s cold-chain design, a temperature breach makes the contract hold the shipment or raise an alert²⁰.

MediLedger deserves a closer look because, unlike the other entries, it ran with real companies rather than in a lab. The pilot showed that major manufacturers and distributors could verify DSCSA events on a permissioned blockchain without disclosing proprietary information to one another¹³. Technically the system performed as intended. Adoption still slowed, and the obstacles proved organisational rather than technical. Onboarding legacy systems was complex, and no

universal data standard emerged to ease that work. Coordinating governance among competing commercial entities carried its own overhead¹⁴. The scope stayed narrow as well, covering DSCSA serialisation rather than full supply chain traceability.

Limitations and Deficits in the Current Literature

Absence of real-world empirical testing

Proposed frameworks have been validated in small pilots or simulations, almost never in live pharmaceutical supply chains^{9,16}. Their scaling behaviour and their durability under operational conditions are therefore unknown. The present study does not escape this limitation and frames itself as a conceptual design for that reason.

Privacy and data security risks

Even on a permissioned network, firms are reluctant to expose detailed supply chain data to their competitors⁹. The IoT devices introduce a second privacy problem. A cheap sensor or tag with weak security can be tampered with or spoofed. Once a false reading reaches the ledger, the same design that stops records being erased also stops it being removed²³. Many papers name zero-knowledge proofs and strict data minimisation as remedies. The proposed designs rarely specify how either would be built in.

Integration difficulties

Integration receives even less attention. Few papers explain how a blockchain and IoT system would connect to existing enterprise resource planning software or barcode-based workflows²⁴, or how it would honour established data standards

Table 1 Comparative overview of blockchain-based pharmaceutical supply chain frameworks.

Framework / System	Blockchain Platform	Key Privacy Features	Reported Throughput	Limitations Noted
PharmaChain ²¹	Hyperledger Fabric	Role-based access; channel separation	Not quantified	Deployment complexity; no cost analysis
MediLedger ¹³	Permissioned Ethereum	Zero-knowledge proofs; privacy-preserving verification	Not quantified	Scope limited to DSCSA; onboarding barriers
Jamil et al. ²²	Hyperledger Fabric	Encryption at rest; consortium access	Not quantified	Hospital-scale only; no IoT integration
Nawale et al. ¹⁹	Not specified	Permissioned access; RFID identity binding	Not quantified	Conceptual; no deployment
Singh et al. ²⁰	IoT-blockchain prototype	Off-chain sensitive data	Demonstration only	Limited to temperature use case
This study	Permissioned consortium (Fabric-inspired)	Role-based access; off-chain sensitive data; signed handoffs	Literature-derived expected range	Conceptual; no implementation

such as GS1 product identifiers¹⁴. A pharmaceutical firm cannot replace its existing systems overnight, and without a described migration path the proposals give it nowhere to start.

Scalability limitations

Scalability is the one limitation where published measurements are specific enough to compare against pharmaceutical workloads. On a research testbed, standard Hyperledger Fabric handled about 3,000 transactions per second (TPS), and the same team later re-engineered it to reach 20,000 TPS²⁵. Another group ran Fabric on a single cloud server with up to 100,000 participants²⁶. A national pharmaceutical network must record an event at every change of ownership for every saleable unit, and a cold-chain deployment adds a continuous stream of sensor readings on top of that. Most published pharmaceutical prototypes report throughput from configurations far smaller than a real deployment would require, and neither peak loads nor multi-year ledger growth has been tested at anything approaching that volume. How these systems behave at national or global scale is therefore uncharacterised.

Limited cost-benefit analysis

Few studies evaluate whether the systems they propose would be economically viable⁵. Running validator nodes and tagging very large numbers of individual packages carry real expense, and upgrading legacy IT systems adds more. The offsetting benefits, such as reduced counterfeiting and faster recalls, are rarely weighed against those costs⁵. Much of the cost discussion that does exist is framed in public-blockchain terms. Pharmaceutical designs built on public Ethereum report their costs as gas fees, and a systematic review of the field lists high gas costs among the limitations of the studies it examined^{10,16}. Because permissioned networks charge no such fees, those figures cannot be carried over to a permissioned deployment. Section "Cost Considerations under a Permissioned Architecture" sets out a cost basis suited to permissioned infrastructure.

Research Gap

Among the frameworks reviewed here, none combines a specification detailed enough to build with evidence from a real deployment. The limitations reviewed above set four requirements for closing that gap. An architecture must be specified in enough detail that another researcher could build it. Privacy must be designed into the data model from the start rather than appended as a later concern. Costs must be framed for permissioned infrastructure instead of borrowed from public-network gas economics, and performance claims must stay within what the cited benchmarks actually support. This study addresses those four requirements as a conceptual contribution.

Methods

Research Approach and Justification

This study designs the system conceptually rather than building it. The work specifies the architecture in detail and evaluates the smart-contract logic by walking representative scenarios through it.

A live pharmaceutical distribution network was not available for research, and regulatory and confidentiality barriers rule out such access at this stage of design. A meaningful prototype would also require a consortium of real organisations that an individual researcher cannot assemble. Much of the published work on pharmaceutical blockchain systems likewise consists of proof-of-concept frameworks evaluated before any live deployment¹⁶. The research questions follow those limits, asking whether the architecture holds together and whether its contract logic enforces the intended rules in representative scenarios. Beyond that, the study asks only what published benchmarks suggest about plausible performance.

Two alternative methods were considered and rejected. A case study of an existing deployment cannot evaluate an architecture that does not yet exist anywhere. An experimental deployment in a real pharmaceutical environment would answer the most useful questions but exceeds the resources available to this project.

System Architecture

The system has four layers, shown in Figure 2. The Device Layer, at the bottom, holds the hardware installed at each supply chain node. Temperature and humidity sensors sit alongside the RFID readers, NFC labels, and QR code scanners that identify each product. Above it, the Gateway and Middleware Layer authenticates each contributing device and packages its readings as structured transactions for submission to the blockchain network through a secure API over TLS. Next comes the Blockchain Layer, a permissioned consortium network modelled on Hyperledger Fabric. Manufacturers, wholesalers, distributors, and pharmacies each run a validator node, and a PBFT-style consensus protocol commits an entry only after those nodes agree on it. The layer also holds the smart contracts, called chaincode on that platform. They carry every transfer-validation and condition-monitoring rule in the system. The Application Layer at the top gives each role its own dashboard for looking up traceability records and watching shipments and alerts. Information moves upward through the stack, and nothing is written to the ledger until a smart contract has validated it.

Stakeholder Modelling

Stakeholder modelling here means choosing which supply chain roles the design must represent. This is actor modelling, not statistical sampling of a population. Roles were selected so that the architecture covers every custody transition from manufacturing to dispensing. The design models four actor categories.

- The Manufacturer opens the chain by entering a batch record for each production lot.
- The Wholesaler receives batches directly from the manufacturer and logs receipt with quality checks.
- The Distributor moves goods from wholesaler to pharmacies, standing in for the intermediate transport and storage stages.
- The Pharmacy receives shipments and records the final sale or dispensing event.

These categories match the standard regulatory definitions of supply chain participants under U.S. DSCSA and international distribution frameworks¹⁴. For tractability, the walk-through analysis models a linear flow from one Manufacturer to one Wholesaler to one Distributor to one Pharmacy. Real supply chains branch into several distributors and pharmacies per lineage, and the design has not been extended to those configurations.

Data Model and Event Taxonomy

The data model covers four kinds of supply chain event. Product handoffs form the core record. Every entry holds a unique product identifier (a serial number or RFID tag) along with the parties involved, the time of the handoff, and a digital signature. Identification scans confirm provenance whenever an IoT device reads a product at a checkpoint. In transit, sensors log temperature in degrees Celsius and relative humidity as a percentage, and cold-chain shipments are held to the 2 to 8 degree range set out in WHO guidance²⁷. The fourth category is location, captured as GPS coordinates and a synchronised timestamp whenever a shipment arrives at or leaves a node.

The event taxonomy follows the records that regulation requires rather than any single data source. The FDA DSCSA specifies the transaction information that must accompany every change of ownership at package level, and that requirement fixes the fields each handoff record carries¹⁴. WHO cold-chain guidance sets the temperature range against which transit readings are checked. No operational dataset was processed or analysed in this study.

Every field in the model describes the product rather than a person. It stores identifiers, storage conditions, locations, and timestamps. No patient or personal data enters any layer of the architecture.

Smart Contract Logic Specification

Before recording any handoff, a smart contract must verify three conditions: (i) a valid batch identifier present on the authorised product ledger; (ii) a valid digital signature from an authorised actor; and (iii) a continuous chain-of-custody link to the prior transaction. Each monitored condition has its own threshold rule, and for cold-chain goods the temperature must stay between 2 and 8 degrees Celsius. A reading outside the allowed range flags the affected batch automatically and alerts permissioned stakeholders.

Role-based access control runs through the same contracts. Each role may write only the events belonging to its own stage. A Manufacturer node logs batch creation and a Wholesaler node logs receipt from the manufacturer, while Distributor and Pharmacy nodes log onward shipment and dispensing respectively. The contract rejects any write that falls outside the submitting node's role. These rules exist as a specification rather than as implemented code, and Section "Smart Contract Logic Correctness: Walkthrough Analysis" evaluates them by scenario walkthrough.

Compliance Benchmarking Framework

The design is tested against two regulatory standards. WHO cold-chain guidance sets the temperature ranges for biological products and expects them to be monitored for the whole of

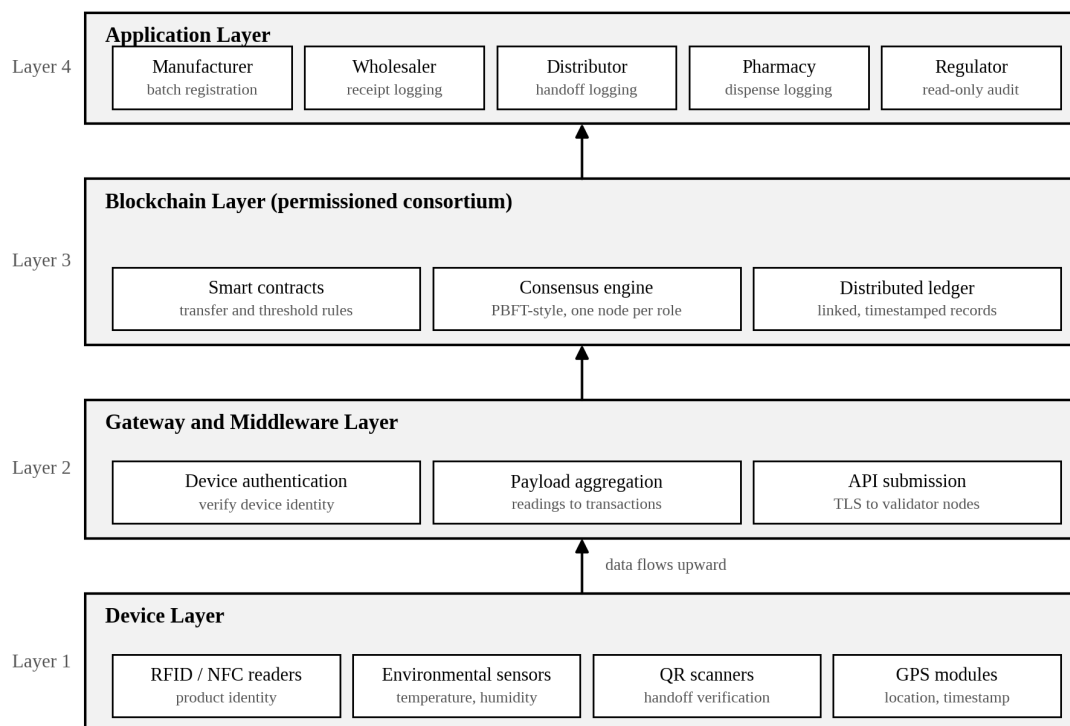


Figure. 2 Four-layer system architecture of the proposed framework

transit²⁷. Under the FDA Drug Supply Chain Security Act (DSCSA), each package must be traceable electronically, in a form that other trading partners' systems can read¹⁴. Each requirement is then paired with the part of the architecture that meets it, and Section "WHO and FDA Compliance Mapping" lays out the full mapping.

Expected-Performance Analysis Approach

Every performance figure in this paper comes from published measurements of other systems. Unmodified Hyperledger Fabric has been measured at about 3,000 TPS on a research testbed, and a re-engineered version at up to 20,000 TPS²⁵. A single cloud instance has supported up to 100,000 participants²⁶. Section "Expected Performance Ranges from Comparable Published Systems" reports these as expected ranges for the proposed framework and labels them literature-derived wherever they appear. The proposed system itself was never built, and none of these figures is a measurement of it.

Ethical Considerations

Because the study used no human subjects and no personal data, it did not need Institutional Review Board approval.

In the design, only product data goes on the blockchain. Business-sensitive and personal identifiers are kept off-chain or anonymised. Consortium members must also agree on who can see what, and on how the network is governed, before the first record is written. After a recall or tampering incident, liability can be traced through signed, timestamped ledger entries rather than assigned by inference. Running the system for real would add formal agreements between the participating companies and regular privacy impact assessments under whatever data protection law applies.

Results

Architectural Feasibility Assessment

Following one sensor reading through the stack shows that every handoff between layers is defined. The reading starts in the Device Layer. The Gateway and Middleware Layer authenticates the device and packages the reading, the Blockchain Layer validates and commits it, and authorised users then view it on an Application Layer dashboard. No path in the design lets data from any device or actor reach the ledger without passing the same contract validation.

Commercially sensitive attributes stay off-chain, and the ledger holds only a cryptographic hash of each. That answers the privacy concern raised in Section "Privacy and data security risks". Legacy systems already work with GS1 identifiers, and the data model adopts that standard for product identifiers (Section "Integration difficulties"). Regulators receive read-only access to custody records through an audit dashboard in the Application Layer.

Smart Contract Logic Correctness: Walkthrough Analysis

The contract logic was evaluated by stepping five representative scenarios through the specifications rather than by executing code in a prototype. The scenarios were chosen so that each verification condition in Section "Smart Contract Logic Specification" is exercised at least once, covering a valid transfer, two distinct grounds for rejection, a sensor-triggered condition, and a read query rather than a write.

1. Authorised manufacturer-to-wholesaler transfer. The contract receives a valid batch identifier with a manufacturer signature and a wholesaler node receipt. All three verification conditions in Section "Smart Contract Logic Specification" pass, and the contract records the transfer as a new entry linked to the batch creation record.
2. Unauthorised actor attempting to log a transfer. A node whose role does not match the handoff stage tries to write the transfer. The contract rejects it under the role rules in Section "Smart Contract Logic Specification" and logs an error.
3. Mismatched batch identifier. The transfer references a batch absent from the authorised product ledger. It fails condition (i) and is rejected.
4. Cold-chain temperature excursion. When a sensor reading on a cold-chain shipment falls outside 2 to 8 degrees Celsius, the threshold rule flags the affected batch and alerts permissioned stakeholders.
5. End-to-end batch lineage retrieval. The ledger's linkage structure answers a query for one batch's full custody history with an unbroken chain of timestamped, signed events from manufacture to dispensing.

In all five walkthroughs, the contract produced the outcome its specification requires. That result is evidence of specification correctness and nothing more. The walkthroughs are not a security evaluation. They do not test adversarial inputs crafted to evade validation, replay attacks, spoofed IoT sensors, or Sybil attacks. A formal security evaluation, including penetration testing and verification of the contract code, must precede any real-world deployment.

WHO and FDA Compliance Mapping

Table 2 sets each compliance requirement, drawn from WHO cold-chain guidance and the FDA DSCSA, against the design feature that answers it. Each requirement examined corre-

Table 2 Compliance mapping between WHO and FDA requirements and design features.

Compliance Requirement	Re-	Source	Design Feature That Addresses It
Authorised-handoff verification		FDA DSCSA package-level traceability ¹⁴	Role-based smart-contract validation; rejection of writes from unauthorised actor nodes (Section "Smart Contract Logic Specification")
Interoperable electronic tracing	elec-	FDA DSCSA ¹⁴	GS1-compatible product identifiers stored on ledger; permissioned consortium with shared schema (Section "System Architecture")
Chain-of-custody continuity		FDA DSCSA ¹⁴	Cryptographically linked, timestamped immutable ledger entries at every hand-off (Section "System Architecture")
Cold-chain temperature monitoring	tempera-	WHO cold-chain guidance ²⁷	IoT temperature sensors at each node; smart-contract threshold rules with automated flagging (Data Model and Event Taxonomy and Section "Smart Contract Logic Specification")
Tamper-evident record-keeping		WHO falsified-products guidance ¹	Immutable distributed ledger; cryptographic hash linkage; consensus across validator nodes (Section "System Architecture")
Privacy of proprietary attributes		Industry concern about data sharing ²⁴	Off-chain storage of sensitive attributes; only cryptographic hashes anchored on-chain (Section "System Architecture")

sponds to at least one design feature. This mapping does not constitute a regulatory certification. Before any real-world deployment, the relevant authorities would still need to review the system formally, and the system would need to demonstrate compliance on operational data.

Expected Performance Ranges from Comparable Published Systems

Table 3 reports expected ranges assembled from published benchmarks of comparable permissioned blockchain systems. Every numerical value comes from the published source cited beside it. The two qualitative rows refer back to the walkthroughs in Section "Smart Contract Logic Correctness: Walkthrough Analysis". None of the entries is a measurement of the proposed framework.

Taken together, the published ranges suggest that a Fabric-inspired build of this framework could handle moderate-scale supply chain workloads. National or global event volumes would require further architectural work. Batching transactions and moving bulk sensor data off-chain would both reduce the load on the ledger, and sharding would go further at the cost of added complexity. None of these options has been tested here.

Table 3 Expected performance ranges based on published benchmarks of comparable permissioned blockchain systems.

Performance Metric	Expected Range	Unit	Source
Transaction throughput (unmodified Fabric, research testbed)	about 3,000	TPS	25
Transaction throughput (re-engineered Fabric)	up to 20,000	TPS	25
Participants supported (single cloud instance)	up to 100,000	participants	26
Invalid transaction rejection (specification-correctness)	all unauthorised transfers rejected by walkthrough	qualitative	Section "Smart Contract Logic Correctness: Walk-through Analysis"
End-to-end trace retrieval	supported by ledger linkage structure	qualitative	Section "Smart Contract Logic Correctness: Walk-through Analysis"

Cost Considerations under a Permissioned Architecture

Permissioned blockchains do not charge gas fees. Gas is how public networks such as Ethereum pay the validators who process transactions and deter spam. In a permissioned consortium, the validators are the member organisations themselves. Each runs its own nodes, and no per-transaction fee changes hands. Pricing a permissioned system with a gas-fee model is therefore a category error, and the gas-based figures reported for public-chain designs (Section "Limited cost-benefit analysis") cannot be reused for it. A permissioned deployment pays for infrastructure and operations instead.

Cloud hosting for each validator node runs on the order of tens to low hundreds of US dollars per month, judging by current on-demand pricing for comparable virtual machines²⁸. Storage cost rises with the volume of data kept on-chain, and the design keeps bulk sensor readings off-chain partly for that reason. Maintenance adds the staff time needed to operate nodes and to update software and contracts as regulations change. IoT hardware cost depends on how many nodes are fitted with sensors and readers, and of which type. A full cost-benefit comparison against conventional track-and-trace systems is beyond a conceptual study and remains a priority for future empirical research.

Discussion

Interpretation of the Conceptual Framework

The results support the architecture as a specification but say nothing about its behaviour under real operating conditions.

Neither technology solves the traceability problem alone. A ledger gives competing stakeholders an audit trail that no single party can edit, but it records only what it is told. With sensors writing directly to the ledger, the record shows both who held a shipment and whether it stayed within temperature limits. Role-based access control and off-chain storage keep that shared record from exposing commercially sensitive data to competitors.

Comparison with Prior Work

The design agrees with prior work on its main choices. Most proposals in the literature adopt a permissioned ledger for pharmaceutical applications^{19,21}, and the use of smart contracts to automate transfer validation and condition monitoring follows Singh et al. and Nawale et al.^{19,20}. Its approach to keeping commercially sensitive data off the shared record also follows earlier pharmaceutical designs, including Musamih et al. and the MediLedger pilot^{10,13}.

Where earlier studies extrapolate from small simulations toward national-scale claims, this study limits its conclusions to what a conceptual design and literature synthesis can establish. It also uses a permissioned cost model throughout, rather than the gas-fee pricing described in Section "Limited cost-benefit analysis".

Limitations of This Study

The study has six limitations:

- Nothing was implemented. Every finding comes from specification, walkthrough, compliance mapping, or the published literature.
- The performance ranges come from published benchmarks of comparable permissioned deployments and describe those systems rather than this framework.
- A walkthrough tests whether a specification is internally correct, not whether it resists attack. The five scenarios say nothing about adversarial inputs.
- The modelled topology is a straight line from one Manufacturer to one Wholesaler to one Distributor to one Pharmacy. Real chains branch, and branching may introduce complexity that the linear model does not capture.

- Cost figures are rough estimates drawn from general cloud pricing, and no rigorous cost-benefit analysis has been carried out.
- Legacy integration was outlined but not engineered. The interfaces to existing enterprise systems and GS1 workflows are not specified at implementation depth.

Recommendations for Future Research

The conceptual work points to four empirical next steps:

- Build the prototype. Implementing the four-layer architecture on a Hyperledger Fabric testnet and running the contract logic against synthetic and operational datasets would replace every literature-derived range in this paper with a measurement. Extending that build to multi-branch topologies, with several distributors and pharmacies per shipment lineage, would then characterise scalability under realistic branching.
- Run a pilot with real participants, from a manufacturer at one end of the chain to a dispensing pharmacy at the other. A pilot would test the architectural assumptions against operational conditions. It would also expose legacy-integration questions that no testnet can, including GS1 serialisation compatibility and links to existing enterprise resource planning systems.
- Test the contracts against the attacks that Section "Smart Contract Logic Correctness: Walkthrough Analysis" left out. Adversarial inputs and spoofed sensors are the obvious place to start, and formal verification of the contract code would follow.
- Model the full economics. The literature still lacks a comparison of blockchain and IoT adoption against conventional pharmaceutical track-and-trace that covers both implementation and ongoing operation.

Conclusion

This study specified a four-layer permissioned blockchain and IoT architecture for pharmaceutical supply chain traceability. Walking its smart-contract logic through five representative scenarios showed the contracts enforcing the intended custody and temperature rules. Each WHO and FDA requirement examined maps onto a specific design feature. The cost model is built for permissioned infrastructure instead of public-chain gas fees, and every performance figure comes from published benchmarks of other systems.

Nothing was built, and no measurements were taken. The walkthroughs checked the specification for internal correctness but did not test the system against attack, and the cost

figures remain estimates until a full cost-benefit analysis is done.

The next step is to build the system on a Hyperledger Fabric testnet and measure it. A pilot with real manufacturers, wholesalers, distributors, and pharmacies should follow. Whether a permissioned ledger can keep falsified medicines out of the supply chain is a question only a working system can answer. This paper provides the architecture and contract logic such a system would need, with the legacy interfaces still to be specified.

References

- 1 World Health Organization. Substandard and falsified medical products. WHO Fact Sheet, 2017, <https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products>.
- 2 World Health Organization. A study on the public health and socioeconomic impact of substandard and falsified medical products. WHO, 2017, <https://www.who.int/publications/i/item/9789241513432>.
- 3 Pharmaceutical Technology. MHRA renews recall of counterfeit Lipitor. Pharmaceutical Technology, 2006, <https://www.pharmtech.com/view/mhra-renews-recall-counterfeit-lipitor>.
- 4 Pfizer Inc. Case study: Lipitor UK recall. Pfizer, 2007, <https://cdn.pfizer.com/pfizercom/products/LipitorUKRecall.pdf>.
- 5 N. Kshetri. Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*. Vol. 39, pg. 80–89, 2018, <https://doi.org/10.1016/j.ijinfomgt.2017.12.005>.
- 6 E. Tijan, S. Aksentijevic, K. Ivanic, M. Jardas. Blockchain technology implementation in logistics. *Sustainability*. Vol. 11, pg. 1185, 2019, <https://doi.org/10.3390/su11041185>.
- 7 S. A. Abeyratne, R. P. Monfared. Blockchain ready manufacturing supply chain using distributed ledger. *International Journal of Research in Engineering and Technology*. Vol. 5, pg. 1–10, 2016, <https://doi.org/10.15623/ijret.2016.0509001>.
- 8 M. Barratt, A. Oke. Antecedents of supply chain visibility in retail supply chains: a resource-based theory perspective. *Journal of Operations Management*. Vol. 25, pg. 1217–1233, 2007, <https://doi.org/10.1016/j.jom.2007.01.003>.
- 9 K. A. Clauson, E. A. Breeden, C. Davidson, T. K. Mackey. Leveraging blockchain technology to enhance supply chain management in healthcare. *Blockchain in Healthcare Today*. Vol. 1, 2018, <https://doi.org/10.30953/bhty.v1.20>.
- 10 A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, S. Ellahham. A blockchain-based approach for drug traceability in healthcare supply chain. *IEEE Access*. Vol. 9, pg. 9728–9743, 2021, <https://doi.org/10.1109/ACCESS.2021.3049920>.
- 11 K. M. Botcha, V. V. Chakravarthy, A. Anurag. Enhancing traceability in pharmaceutical supply chain using internet of things (IoT) and blockchain. 2019 IEEE International Conference on Intelligent Systems and Green Technology (ICISGT). pg. 45–48, 2019, <https://doi.org/10.1109/ICISGT44072.2019.00025>.
- 12 M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, J. H. Kek. Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains. *IEEE Access*. Vol. 7, pg. 7273–7285, 2019, <https://doi.org/10.1109/ACCESS.2018.2890389>.
- 13 MediLedger Project. MediLedger DSCSA pilot project final report. U.S.

-
- Food and Drug Administration, 2020, <https://www.fda.gov/media/168283/download>.
- 14 U.S. Food and Drug Administration. Drug supply chain security act (DSCSA). FDA, 2023, <https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa>.
 - 15 P. Dutta, T. M. Choi, S. Somani, R. Butala. Blockchain technology in supply chain operations: applications, challenges and research opportunities. *Transportation Research Part E*. Vol. 142, pg. 102067, 2020, <https://doi.org/10.1016/j.tre.2020.102067>.
 - 16 N. Zakari, M. Al-Razgan, A. Alsaadi, H. Alshareef, H. Al saigh, L. Alashaikh, M. Alharbi, R. Alomar, S. Alotaibi. Blockchain technology in the pharmaceutical industry: a systematic review. *PeerJ Computer Science*. Vol. 8, pg. e840, 2022, <https://doi.org/10.7717/peerj-cs.840>.
 - 17 J. H. Tseng, Y. C. Liao, B. Chong, S. W. Liao. Governance on the drug supply chain via Gcoin blockchain. *International Journal of Environmental Research and Public Health*. Vol. 15, pg. 1055, 2018, <https://doi.org/10.3390/ijerph15061055>.
 - 18 M. Uddin, K. Salah, R. Jayaraman, S. Pesic, S. Ellahham. Blockchain for drug traceability: architectures and open challenges. *Health Informatics Journal*. Vol. 27, 2021, <https://doi.org/10.1177/14604582211011228>.
 - 19 S. D. Nawale, R. R. Konapure. Blockchain IoT based drugs traceability for pharma industry. 2021 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC). pg. 1–4, 2021, <https://ieeexplore.ieee.org/abstract/document/9570251>.
 - 20 R. Singh, A. D. Dwivedi, G. Srivastava. Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. *Sensors*. Vol. 20, pg. 3951, 2020, <https://doi.org/10.3390/s20143951>.
 - 21 S. S. Gomasta, A. Dhali, T. Tahlil, M. M. Anwar, A. B. M. S. Ali. PharmaChain: blockchain-based drug supply chain provenance verification system. *Heliyon*. Vol. 9, pg. e17957, 2023, <https://doi.org/10.1016/j.heliyon.2023.e17957>.
 - 22 F. Jamil, L. Hang, K. Kim, D. Kim. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. *Electronics*. Vol. 8, pg. 505, 2019, <https://doi.org/10.3390/electronic8050505>.
 - 23 M. A. Khan, K. Salah. IoT security: review, blockchain solutions, and open challenges. *Future Generation Computer Systems*. Vol. 82, pg. 395–411, 2018, <https://doi.org/10.1016/j.future.2017.11.022>.
 - 24 S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen. Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*. Vol. 57, pg. 2117–2135, 2019, <https://doi.org/10.1080/00207543.2018.1533261>.
 - 25 C. Gorenflo, S. Lee, L. Golab, S. Keshav. FastFabric: scaling Hyperledger Fabric to 20 000 transactions per second. *International Journal of Network Management*. Vol. 30, pg. e2099, 2020, <https://doi.org/10.1002/nem.2099>.
 - 26 M. Kuzlu, M. Pipattanasomporn, L. Gurses, S. Rahman. Performance analysis of a Hyperledger Fabric blockchain framework: throughput, latency and scalability. 2019 IEEE International Conference on Blockchain (Blockchain). pg. 536–540, 2019, <https://doi.org/10.1109/Blockchain.2019.00003>.
 - 27 World Health Organization. Model guidance for the storage and transport of time- and temperature-sensitive pharmaceutical products. WHO Technical Report Series No. 961, Annex 9, 2011, <https://www.who.int/publications/m/item/trs961-annex9>.
 - 28 Amazon Web Services. Amazon EC2 on-demand pricing. AWS, 2026, <https://aws.amazon.com/ec2/pricing/on-demand/>.