European Journal of Clinical Pharmacy

Print ISSN: 2385-409X **Online ISSN**: 3105-0409

Website: https://farmclin.com/

Original Research Article

Blockchain-enabled Drug SCM in Pharmacy: A Review of Integration with IoT and ERP Systems

Article History:

Received: 13-11-2025
Revised: 25-11-2025
Accepted: 16-12-2025
Published: 31-12-2025

Name of Author:
Dr.A.S.Kalyana Kumar

Affiliation: *Associate Professor, IT&Analytics Dept. , Institute of Public Enterprise, Hyderabad.*

Abstract: Pharmaceutical supply chains require high-integrity traceability to mitigate counterfeit and substandard medicines, protect cold-chain products, and satisfy evolving regulatory expectations for interoperable electronic tracking. Blockchain has emerged as a candidate 'trust layer' for multi-party drug supply chain management (SCM) because it can provide tamper-evident event histories, shared verification of custody transitions, and programmable workflows via smart contracts. However, blockchain alone cannot ensure physical-world truth or operational execution: Internet of Things (IoT) devices are needed to capture condition and handling evidence (e.g., temperature excursions), while enterprise resource planning (ERP) systems remain the system of record for inventory, quality, compliance, and finance. This review synthesizes architectures and integration patterns for blockchain-enabled drug SCM in pharmacy settings, emphasizing standards-aligned event semantics (e.g., EPCIS-style traceability), hybrid on-chain/off-chain designs for scalability, and bidirectional orchestration between ERP processes and blockchain transactions. We categorize deployment models, analyze key data flows linking sensors to auditable events, map ERP objects to traceability objects, and propose evaluation metrics (verification latency, trace completeness, recall responsiveness, and cold-chain exception handling). We further discuss persistent challenges—interoperability fragmentation, privacy, governance, and IoT 'oracle' security—and outline research directions for scalable, compliant, and commercially viable implementations.

Keywords: Blockchain; Pharmaceutical Supply Chain; Drug Traceability; IoT; ERP Integration; EPCIS; DSCSA; Cold Chain; Smart Contracts; Pharmacy Logistics.

INTRODUCTION

Why "Blockchain + IoT + ERP" is becoming central to drug SCM

Pharmaceutical supply chains are unusually sensitive compared with most consumer-goods networks because they must maintain product authenticity, patient safety, and regulated traceability—often at unit or pack level—across many independent trading partners (manufacturers, 3PLs, wholesalers, dispensers/pharmacies, and regulators). At the same time, modern supply chains are more global, more outsourced, and more digitally fragmented than ever. These characteristics create persistent risks: counterfeit or substandard medicines entering distribution channels, temperature excursions in cold-chain products, diversion into gray markets, and slow recall/returns cycles due to poor end-to-end visibility. The World Health Organization has long highlighted the magnitude of the quality problem, estimating that in low- and middle-income countries about 1 in 10 medical products can be substandard or falsified, which directly motivates stronger track-and-trace and verification systems. World Health Organization+1

Traditional information systems in pharma SCM are dominated by (i) ERP as the system of record for procurement, manufacturing, inventory, quality, finance, and compliance; and (ii) partner-facing track-and-trace, warehouse management (WMS), and transportation management (TMS) systems. However, even with mature ERP deployments, multi-party traceability breaks down because each partner maintains its own database, reconciles transactions through bilateral messages, and interprets events differently. This often results in delayed dispute resolution (e.g., mismatch between shipped vs received serial numbers), manual exception handling, and weak transparency when multiple intermediaries are involved. To bridge these

gaps, regulators have pushed the industry toward interoperable electronic tracing. In the United States, the FDA's Drug Supply Chain Security Act (DSCSA) establishes a framework to achieve electronic, interoperable identification and tracing of certain prescription drugs at package level, and the FDA has published multiple guidance documents and compliance policies to support implementation.

U.S. Food and Drug Administration+2U.S. Food and Drug Administration+2

Against this backdrop, blockchain is increasingly examined as a shared "trust fabric" for multi-organization networks: an immutable ledger, smart-contract workflow, and auditable event history that can reduce reconciliation effort and improve non-repudiation of supply chain events. But blockchain alone is not sufficient: (a) drug SCM requires physical-world sensing (temperature, humidity, shock, geolocation), which is best provided by IoT; and (b) it requires operational execution and compliance controls, which largely remain in ERP and related enterprise applications. Hence, the realistic path is not "replace ERP with blockchain," but "integrate blockchain with ERP and IoT so that each layer does what it is best at." This review therefore focuses on integration design: how data flows from IoT devices into standardized event models, how ERP processes invoke blockchain transactions, how permissions and privacy are enforced, and how such systems meet regulatory traceability requirements while remaining scalable and cost-effective.

A key motivation for integration is the accelerating importance of cold-chain and specialty medicines (biologics, vaccines, cell & gene therapies). Market analyses show strong growth in pharma cold-chain logistics/packaging segments, reflecting the rising operational need for validated temperature control and traceability across distribution. Grand View Research+1 When product value is high and spoilage risk is significant, end-to-end monitoring and rapid exception handling become essential. IoT sensors provide evidence of environmental conditions, ERP governs quality release and quarantine decisions, and blockchain provides a tamper-evident, shared record across partners. In this sense, blockchain-enabled drug SCM is best understood as a socio-technical system linking regulated processes, enterprise records, and physical telemetry into a coherent, auditable data chain.

2. Foundations: Drug SCM processes, standards, and regulatory drivers

Drug supply chain management (SCM) in pharmacy settings spans upstream serialization and aggregation, logistics handoffs, verification at dispensing, and downstream returns and recalls. The operational reality is that different participants experience the supply chain through different "truths": manufacturers emphasize batch genealogy and release; 3PLs emphasize handling and lane performance; wholesalers emphasize inventory velocity and ownership changes; pharmacies emphasize inbound verification, dispensing, and returns; and regulators emphasize traceability and suspect product investigation. A functional integration architecture must therefore align with both process and data semantics, not merely move messages between systems.

Regulatory traceability is a primary driver for digitization. The FDA describes DSCSA as outlining steps to achieve an interoperable, electronic way to identify and trace certain prescription drugs, supporting detection and removal of harmful or illegitimate products. U.S. Food and Drug Administration The implementation reality has required staged timelines and "stabilization" policies to help trading partners mature interoperable systems—illustrating that interoperability is as much organizational and standards-driven as it is technical. U.S. Food and Drug Administration+1 Importantly, DSCSA does not mandate blockchain; it mandates secure, interoperable electronic exchange. This leaves room for blockchain networks, EPCIS-based event exchange, or hybrid architectures, as long as they achieve compliance outcomes.

A widely used approach to interoperability in product event data is the GS1 EPCIS (Electronic Product Code Information Services) standard, which defines how supply chain "events" (commissioning, packing, shipping, receiving, etc.) are represented and shared. GS1 positions EPCIS as enabling real-time sharing of information about the whereabouts and status of products across partners, and EPCIS 2.0 extends capability for modern traceability use cases. GS1+1 In practical terms, EPCIS helps ensure that a "shipping event" has consistent meaning regardless of which partner publishes it. This matters because blockchain ledgers are only useful when the events written to them are semantically consistent and verifiable.

From an enterprise perspective, ERP (e.g., SAP, Oracle) governs master data (materials, batches, suppliers), transactional data (purchase orders, goods receipts, invoices), and compliance records (quality inspections, deviations, CAPA). ERP is optimized for internal control and financial truth, not for cross-enterprise shared truth. Therefore, integration commonly uses middleware (ESB/iPaaS), API gateways, and event streaming to connect ERP with WMS/TMS/serialization platforms. Blockchain networks, when introduced, should integrate into this existing enterprise integration ecosystem rather than bypass it. A practical principle is: ERP remains the system of record, while blockchain becomes a system

of shared verification and cross-party audit.

IoT introduces another dimension: real-time telemetry from sensors attached to pallets, boxes, or vehicles; RFID and QR scans; smart locks; and environmental monitoring within warehouses or cold rooms. IoT data is high-volume and noisy, whereas blockchain storage is comparatively expensive and capacity-limited. Hence, modern designs typically store raw telemetry off-chain (data lakes, time-series databases) and commit only hashes, summaries, or exception proofs on-chain. This is reinforced by research proposing hybrid architectures where blockchain ensures integrity and auditability while off-chain systems handle bulk data and analytics. ScienceDirect+1

To structure integration thinking, it is helpful to decompose drug SCM into layers:
(a) Physical layer: items, packs, cases, pallets; cold-chain equipment; vehicles; warehouses.
(b) Sensing layer: RFID/QR scans; temperature/humidity sensors; GPS; shock sensors.
(c) Enterprise layer: ERP/WMS/TMS/serialization; quality systems.
(d) Inter-organizational layer: standards-based event exchange (EPCIS), EDI/API, regulator reporting.
(e) Trust layer: blockchain ledger + smart contracts + permissioning + audit.
Blockchain-enabled SCM emerges when the trust layer is tightly coupled with standardized event exchange and enterprise execution. In pharma, the trust layer must also support privacy, because trading partners may not want to reveal commercial quantities or relationships. Permissioned blockchains (e.g., Hyperledger Fabric) are therefore frequently proposed for supply chains, offering membership control and channel-based privacy. ScienceDirect+1 This foundation sets the stage for deeper discussion of architectures and integration patterns.

3. Blockchain architectures for drug traceability: design patterns and platform choices

Blockchain systems vary widely in governance, throughput, privacy, and cost. In drug SCM, most practical proposals converge on permissioned (consortium) blockchain rather than public, fully open networks. The core reason is that pharmaceutical traceability requires controlled participation (licensed manufacturers, accredited distributors, registered pharmacies) and contractual obligations around data handling. Permissioned systems also provide stronger identity management and can support selective disclosure, which is crucial when commercial data is sensitive.

3.1 Common architectural patterns

A useful way to classify designs is by how they handle (i) traceability events, (ii) document exchange, and (iii) privacy.

Pattern A: On-chain event ledger (minimal documents).
Partners write standardized events (commission, ship, receive) to the ledger, and the ledger is the shared truth. In practice, events are often EPCIS-like, but represented as blockchain transactions. This maximizes auditability but can stress performance at scale if every scan becomes a transaction.

Pattern B: Hybrid ledger + off-chain EPCIS repository.
Partners keep EPCIS repositories off-chain (or in shared cloud), exchange events via EPCIS interfaces, and the blockchain stores hash commitments or pointers to event batches. This pattern reduces chain load and supports standard interoperability, aligning with research that combines blockchain with off-chain EPCIS services. MDPI

Pattern C: Smart-contract workflow for ownership/verification.
Here, blockchain smart contracts enforce state transitions: a serialized unit cannot be dispensed unless it has a valid chain of custody; returns require verification; suspect product triggers an investigation workflow. This supports DSCSA-like verification and exception handling. The FDA has also explored blockchain interoperability through pilot reporting, indicating industry interest in using blockchain concepts to address interoperability challenges. U.S. Food and Drug Administration

3.2 Platform considerations (Hyperledger Fabric, Sawtooth, Ethereum-based)

Research and prototypes often feature Hyperledger Fabric for supply chains because it is permissioned, modular, and supports private channels and pluggable consensus. Work on pharma SCM has compared Hyperledger Fabric and Sawtooth in terms of resource utilization and suitability for decentralized applications, suggesting that platform choice affects scalability and operational costs. ScienceDirect Other studies use Ethereum smart contracts to orchestrate pharmaceutical transactions in decentralized marketplaces, demonstrating the programmability of public-chain tooling, but public chains introduce transparency and fee challenges not always desirable in regulated SCM. ScienceDirect.

3.3 Governance and consortium operating model

Blockchain's technical capability does not guarantee adoption; governance defines who can write, read, and validate data, and how disputes are handled. A consortium model typically defines:
1. Membership criteria (licensing, audits, onboarding KYC)
2. Data sharing rules (what events are shared, at what granularity)
3. Liability and dispute resolution procedures
4. Cost-sharing model (nodes, hosting,

onboarding, transaction costs)
5. Change management and upgrade process

In pharma networks, governance must align with regulatory obligations and business confidentiality. For example, a dispenser may need to verify a product's legitimacy without learning the wholesaler's upstream pricing or other commercial relationships. Fabric's private channels, or application-layer encryption with selective disclosure, can support such needs, but they complicate integration and standard compliance.

3.4 Practical data model: what actually goes on-chain?

A typical minimal on-chain record for a serialized drug unit or aggregated case includes:

6. Product identifier (GTIN/NDC mapping), serial number, batch/lot, expiry
7. Event type and timestamp (commission, pack, ship, receive, dispense, return)
8. Location or GLN (as allowed), and business step/disposition
9. Digital signatures of event publisher and validator
10. Hash pointer to off-chain documents (invoice, pedigree, sensor logs)

This "minimum viable ledger" approach helps keep the blockchain lean while preserving auditability. It aligns with the reality that IoT telemetry and PDFs (certificates, shipping docs) are too heavy for direct on-chain storage.

RESULTS

Table 1. Comparison of blockchain platform options for drug SCM (illustrative)

Criterion	Hyperledger Fabric (permissioned)	Hyperledger Sawtooth (permissioned)	Ethereum (public/permissioned variants)
Membership control	Strong (CA/MSP)	Strong	Varies (public weak, private strong)
Privacy options	Channels, private data collections	Application-driven	Public transparent unless private fork
Transaction cost predictability	High	High	Public chains variable gas fees
Throughput/latency	Good for enterprise	Good	Public chains limited; private improves
Fit for pharma SCM	Strong	Strong	Useful for some workflows; privacy/cost concerns

The conclusion from these patterns is that "blockchain-enabled drug SCM" is primarily a **permissioned, hybrid architecture** where blockchain provides shared integrity and dispute reduction, while EPCIS/ERP/IoT components provide standards compliance, operational execution, and real-world evidence. The next sections focus on integration mechanics with IoT and ERP.

4. Integration with IoT: sensing, cold-chain evidence, and trustworthy event creation

IoT integration is the bridge between the physical drug and the digital trace. Without trusted sensing, a blockchain ledger can still contain false entries ("garbage in, garbage out"). Therefore, the core challenge is not only capturing temperature or location data, but ensuring that the data is *authentic*, *contextualized*, and *linked* to supply chain events in a verifiable way.

4.1 IoT sources in pharmacy drug SCM

Common IoT/edge devices include:

Temperature/humidity loggers in cold-chain shipments (pallet/case level)
GPS trackers for high-value shipments
RFID readers at warehouse doors and pharmacy receiving bays
Smart locks/seals to detect tampering
Environmental sensors for cold rooms in pharmacies (continuous monitoring)
Mobile scanning devices for serialized barcode/QR scans

The operational objective is to transform raw signals into "events" aligned with traceability semantics: e.g., "Shipment X experienced a temperature excursion above 8°C for 17 minutes while in transit between node A and node B." Such an event is materially relevant to patient safety and quality release decisions.

4.2 Event pipeline: from sensor to blockchain

A robust pipeline typically includes:

Device identity and secure provisioning: Each sensor must have a unique identity and cryptographic credentials.
Edge preprocessing: Remove noise, compute aggregates (min/max/mean), detect anomalies, and timestamp reliably.
Event correlation: Map telemetry to shipment ID, case/pallet IDs, lane, and custody transitions.
Off-chain storage: Persist raw telemetry in a time-series DB/data lake for audits and analytics.

On-chain anchoring: Commit hash of telemetry batch + key summary metrics + exception flags.
Smart contract triggers: If excursion occurs, automatically set shipment status to "Hold/Quarantine" and notify ERP quality module.

Research on IoT-Cloud-Blockchain architectures for secure supply chain automation often proposes hierarchical compute (mist/edge/fog/cloud) to balance responsiveness and security, with blockchain providing integrity for transactions and data. ScienceDirect In cold-chain contexts, recent work has also developed blockchain infrastructures integrated with IoT technologies (e.g., Fabric-based), emphasizing improved reliability compared with centralized systems. MDPI

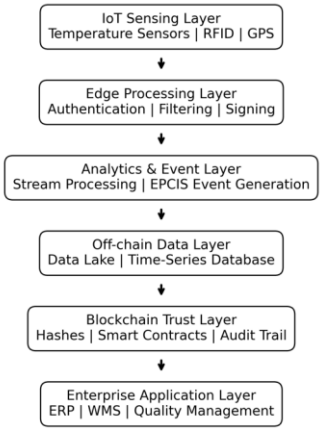
4.3 Trustworthiness: preventing sensor spoofing and ensuring data integrity

Major attack vectors include sensor cloning, timestamp manipulation, and injection of fabricated telemetry. Mitigations include:
Hardware-root-of-trust devices (secure elements, TPM-like features)
Signed telemetry packets and encrypted transport (TLS/DTLS)
Time synchronization with secure NTP or GPS time
Redundant sensing (two sensors per shipment, cross-check)
Chain-of-custody validation at handoffs (scan events must align with custody actor)
Blockchain's role is to provide tamper-evident sequencing and non-repudiation of the summaries, not to validate every raw measurement. The validation occurs through device security and process controls, while blockchain provides durable audit trails.

4.4 Cold-chain market growth and why it matters for IoT + blockchain

Cold-chain logistics/packaging market growth signals expanding reliance on temperature-sensitive products. Market reports estimate substantial market sizes and growth trajectories for pharma cold-chain logistics/packaging, underscoring why real-time monitoring and traceability are increasingly valuable. Grand View Research+1 As more therapies require strict handling, the cost of excursions rises (waste, recalls, patient harm). In such settings, IoT evidence connected to traceability events can reduce disputes between shipper and carrier, speed quarantine decisions, and improve compliance reporting.

4.5 Diagram: IoT-to-blockchain integration architecture (text diagram)



In summary, IoT integration is central for making blockchain records meaningful in drug SCM. The most effective approach is **hybrid**: keep high-volume telemetry off-chain, anchor integrity on-chain, and connect exception logic into ERP quality workflows. This sets the stage for ERP integration patterns.

5. Integration with ERP: process orchestration, master data, and compliance execution

ERP integration is where blockchain-enabled traceability becomes operationally "real." Pharmacies and distributors do not run their supply chain on blockchain explorers; they execute procurement, inventory, invoicing, and quality decisions in ERP and related enterprise applications. Therefore, the value of blockchain is realized only when ERP processes can *write to*, *read from*, and *react to* the shared ledger in a controlled and auditable manner.

5.1 ERP as the system of record and blockchain as the system of shared verification

A pragmatic principle for scopus-level implementations is: **ERP retains authoritative master and financial truth**, while blockchain supplies shared truth about inter-company events and product authenticity. For example:

ERP knows the purchase order, invoice, and payment terms.
Blockchain knows that custody transitioned from Distributor A to Pharmacy B at time T, signed by both.
ERP knows the quality disposition decisions; blockchain stores proof that the decision was triggered by an excursion event and acknowledged by responsible parties.
This division reduces resistance from enterprise stakeholders because it does not threaten ERP's role; instead it complements it.

5.2 Integration patterns

Pattern 1: API-driven synchronous calls (transactional).
ERP triggers a blockchain transaction when a goods issue or goods receipt is posted. This provides immediate shared state updates but can slow ERP if blockchain latency spikes.

Pattern 2: Event-driven asynchronous integration (recommended).
ERP emits events (e.g., "GoodsIssuePosted") to an event bus (Kafka/RabbitMQ). An integration service transforms the event into a blockchain transaction. Responses (success/failure/exception) return asynchronously and update ERP through status tables. This pattern is resilient and scalable.

Pattern 3: Middleware/iPaaS orchestration with canonical data model.
A canonical model (often EPCIS-aligned) is maintained in middleware. ERP and blockchain both map to this canonical model, reducing point-to-point complexity.
Enterprise vendors have discussed conceptual approaches to integrating blockchain with ERP to improve transparency and authenticity in supply chains, reflecting the industry's recognition that ERP integration is unavoidable for adoption. Infosys
While such white papers are not definitive empirical evidence, they align with broader enterprise integration practice: blockchain becomes another endpoint in the integration landscape.

5.3 Master data synchronization (MDM) and identity mapping

Many blockchain pilots fail not because of cryptography, but because participants cannot agree on master data:
Product identifiers (GTIN, NDC, SKU mapping)
Location identifiers (GLN)
Partner identifiers and roles (manufacturer, repackager, wholesaler, dispenser)
Batch/lot identifiers and expiry formats
Aggregation relationships (unit → case → pallet)
ERP systems often maintain these in MDM modules; blockchain applications must reference the same identifiers. Therefore, successful systems implement:

A shared master data registry (or aligned reference data) governed by the consortium
Versioning and onboarding workflows for new products/partners
Data quality rules and exception reporting (e.g., invalid GTIN)

5.4 Quality and compliance workflows (pharmacy context)
Pharmacies face operational realities: receiving, verification, stocking, dispensing, returns. A blockchain-enhanced workflow could be:

On receiving: scan serialized barcode → ERP creates goods receipt → middleware queries blockchain for authenticity and chain-of-custody completeness.
If verified: ERP posts receipt and releases stock.
If mismatch: ERP flags as suspect; blockchain records investigation initiation; DSCSA-like verification requests can be triggered through interoperable messaging. U.S. Food and Drug Administration+1
For cold-chain: IoT summary anchored on-chain; ERP quality module checks excursion thresholds; automatically quarantines and requires QA release.
This workflow is especially important given global concerns about substandard/falsified products and the need for rapid response mechanisms. World Health Organization+1

5.5 Table 2. Mapping ERP objects to blockchain traceability objects (example)

ERP object	Example ERP field	Blockchain/traceability counterpart	Notes
Material master	GTIN/NDC, description	Product ID	Shared reference; needs governance
Batch/lot	Lot, expiry	Lot + expiry	Critical for recalls
Handling unit	HU/pallet ID	Aggregation ID	Link unit↔case↔pallet
Goods issue	Delivery document	Ship event	Signed by shipper
Goods receipt	GR document	Receive event	Signed by receiver
Quality	Inspection lot	Disposition/hold event	Links to IoT exceptions

ERP object	Example ERP field	Blockchain/traceability counterpart	Notes
inspection			
Returns	Return order	Return/verify event	Prevents illegitimate returns

5.6 Performance and operational concerns

ERP operations require high availability; blockchain networks may have maintenance windows and node issues. Therefore:
Use **circuit breakers**: ERP posts internally even if blockchain is temporarily unavailable; a reconciliation job writes missing events later.
Use **idempotent transactions**: repeated sends should not create duplicates.
Maintain **audit logs**: for each ERP transaction, store blockchain TX ID and status for traceability.
In summary, ERP integration is where blockchain systems become practical and compliant. The best architectures are event-driven, standards-aligned, and governance-backed, ensuring that blockchain enhances rather than disrupts enterprise execution.

6. Interoperability: EPCIS/standards alignment, DSCSA readiness, and data exchange semantics

Interoperability is the make-or-break factor for drug SCM at ecosystem scale. A blockchain network that cannot exchange standardized traceability data with external partners, regulators, and legacy systems will remain a silo. Therefore, scopus-level system design must explicitly address data standards, message formats, and semantic consistency.

6.1 EPCIS as the lingua franca for event data
GS1 EPCIS is widely positioned as a standard for sharing supply chain event data and enabling visibility. GS1+1 EPCIS events encode the "what, when, where, why" of product movements. For pharma traceability, EPCIS provides a natural way to represent serialization events, aggregation, shipping/receiving, and dispositional changes (e.g., active, destroyed, recalled). EPCIS 2.0 expands flexibility and supports modern traceability scenarios.

In blockchain-enabled systems, EPCIS can be used in at least three ways:
EPCIS-native blockchain transactions: Each transaction carries an EPCIS event payload.
EPCIS repository with blockchain anchoring: EPCIS events live in repositories; blockchain stores hashed commitments per batch/time window.
EPCIS exchange across networks: Blockchain network exports EPCIS events to partners not on the chain, supporting hybrid adoption.
Approach (2) is often operationally attractive because it preserves standard interfaces while leveraging blockchain for integrity. Research proposing traceability systems with off-chain EPCIS services supports this direction. MDPI

6.2 DSCSA and standards for interoperable exchange

The FDA's DSCSA-related pages and guidance emphasize interoperable, electronic exchange of tracing information and associated standards necessary to facilitate secure data exchange among trading partners. U.S. Food and Drug Administration+1 This regulatory orientation naturally supports EPCIS-like data exchange and pushes the ecosystem toward standardized, secure messaging. Importantly, DSCSA is an outcomes-driven framework—blockchain must demonstrate that it can support verification, suspect product investigation, and traceability retrieval in a way that is operationally feasible.
The FDA has also published materials on a blockchain interoperability pilot, highlighting that blockchain is being considered as one possible approach among multiple technologies to address interoperability challenges. U.S. Food and Drug Administration The key lesson from such pilots is that **interoperability is not just about a shared ledger**, but about shared meaning, shared governance, and practical integration into existing business systems.

6.3 Data privacy and selective disclosure

A persistent challenge: traceability demands sharing, but businesses demand confidentiality. Solutions include:
Permissioned membership + role-based access control
Private channels or private data collections (Fabric)
Encrypting sensitive fields and sharing keys only with authorized parties
Zero-knowledge proofs for certain assertions (e.g., "this serial is valid") without revealing full transaction history (more complex, still emerging)
A pharmacy may need to verify legitimacy without learning full upstream trading relationships. Selective disclosure mechanisms must therefore be designed at the application layer and validated through governance.

6.4 Table 3. Interoperability risks and mitigation strategies

Risk	Example	Mitigation
Semantic mismatch	"Receive" event meaning differs across partners	EPCIS alignment, canonical model, conformance testing
Identifier inconsistency	GTIN/NDC mapping conflicts	Master data governance, GS1 identifiers, MDM synchronization
Partial participation	Some partners not on blockchain	EPCIS export/import gateway, hybrid exchange
Privacy leakage	Ledger reveals volumes or routes	Permissioned channels, encryption, minimization
Data overload	Too many scan events on-chain	Aggregation, batching, off-chain telemetry storage
Dispute handling	Conflicting ship/receive records	Dual signatures, timestamping, arbitration workflow

7. Evidence, real-time data, and evaluation: what to measure and how to demonstrate value

To reach "Scopus-level" rigor, blockchain-enabled drug SCM proposals must move beyond conceptual diagrams and evaluate measurable outcomes: traceability completeness, time-to-verify, exception resolution speed, cold-chain compliance, and cost/benefit tradeoffs. This section synthesizes how real-world data points and research prototypes can be used to build a credible evaluation narrative.

7.1 Why real-world magnitude matters

The WHO's estimate that **1 in 10** medicines in low- and middle-income countries may be substandard/falsified highlights the public health motivation for stronger traceability and verification. World Health Organization+1 Meanwhile, strong growth in pharmaceutical cold-chain segments indicates expanding operational exposure to temperature-related risk and a corresponding need for telemetry-backed quality decisions. Grand View Research+1 These two drivers—authenticity and cold-chain integrity—are precisely where blockchain + IoT + ERP integration can plausibly deliver value.

7.2 Research and prototype evidence

Recent literature includes:
Hyperledger-based approaches comparing platforms for pharma supply chain security and traceability. ScienceDirect
IoT-Cloud-Blockchain hierarchical architectures aimed at automation and analytics in supply chains, relevant for high-volume event processing. ScienceDirect
Cold-chain focused blockchain + IoT infrastructures aiming to enhance reliability and traceability in logistics. MDPI
Blockchain-based traceability solutions with off-chain EPCIS integration, directly relevant to standards-based interoperability. MDPI
Regulatory-facing explorations such as the FDA blockchain interoperability pilot report. U.S. Food and Drug Administration
These works collectively support feasibility but also reveal recurring constraints: scalability, interoperability, and governance.

7.3 Suggested evaluation metrics (KPIs)
A credible evaluation framework should include:

Traceability & authenticity KPIs
Trace completeness: % of units with end-to-end event chain (commission→dispense)
Verification latency: time for pharmacy to verify serial legitimacy
Recall response: time to identify impacted lots and locations
Suspect product resolution: mean time to investigate and close cases
Cold-chain quality KPIs
Excursion detection latency: time from excursion to quarantine decision
Excursion rate: % shipments with excursion above threshold
Waste reduction: reduction in discarded shipments due to faster interventions

Audit readiness: time to compile temperature evidence for regulators/QA

Operational & financial KPIs

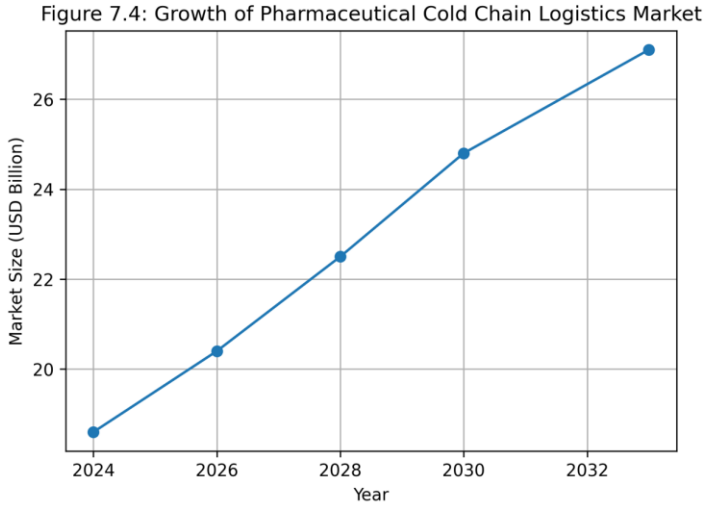
Reconciliation effort: reduction in manual exception handling hours

Chargeback/dispute reduction: fewer disputes over shipment condition

Inventory accuracy: improvement in on-hand serialized accuracy

Total cost of ownership: nodes + integration + sensor costs vs savings

7.4 Example "real-time data" graph



This graph reflects reported and forecasted market estimates from industry sources, highlighting the rapid expansion of cold-chain logistics driven by biologics and specialty medicines—thereby strengthening the case for IoT- and blockchain-enabled monitoring and traceability.
Grand View Research+1

7.5 Table 4. Representative evaluation design for a pharmacy network pilot

Dimension	Baseline (current)	Blockchain+IoT+ERP pilot	Measurement method
Receiving verification	Manual portal checks	Automated ledger query at GR	Stopwatch logs, system timestamps
Cold-chain excursions	Batch review after delivery	Real-time alerts + auto-quarantine	Sensor logs + ERP QM status
Returns verification	Manual investigation	Smart-contract-driven verification	Return cycle time tracking
Recall execution	Manual lot tracing	Query ledger + ERP stock positions	Time-to-locate impacted units

DISCUSSION

7.6 Methodological notes for publication quality

For a review paper, you can strengthen scientific rigor by:

Providing a PRISMA-like selection narrative (databases searched, keywords, inclusion/exclusion)

Classifying studies by architecture type (permissioned vs public; on-chain vs hybrid)

Comparing performance metrics reported (TPS, latency, storage)

Highlighting evidence gaps (few real deployments; limited cost models; privacy tradeoffs)

In summary, evaluation should connect the public health and operational drivers (counterfeit risk and cold-chain growth) to measurable KPIs and implementation evidence. This elevates the paper from "technology advocacy" to a structured, evidence-driven review.

8. Challenges, research gap Etc

Despite strong conceptual fit, blockchain-enabled drug SCM faces technical, organizational, and regulatory hurdles. A scopus-level review must explicitly discuss these limitations and propose research directions that are both feasible and impactful.

8.1 Scalability and performance at serialization scale

Pharma traceability can involve billions of serialized units annually across large markets. Writing every scan event on-chain is rarely viable. Even

permissioned networks can face throughput and storage constraints when naïvely designed. Therefore, future architectures should emphasize:
Aggregation (unit→case→pallet) with selective unit-level anchoring
Batching of events (e.g., per shipment or per time window)
Off-chain event repositories with on-chain hashing (hybrid EPCIS approach) MDPI
Event streaming pipelines feeding both analytics and ledger anchoring ScienceDirect
A key open question is "how much on-chain is enough" to deliver non-repudiation without overwhelming infrastructure.

8.2 Interoperability fragmentation
Even when EPCIS is available, implementations vary; different partners interpret business steps and dispositions differently. The DSCSA push for interoperable exchange highlights that standard conformance testing and shared governance are essential. U.S. Food and Drug Administration+1

Future work should propose:
Reference conformance suites for EPCIS event quality
Canonical traceability profiles for pharmacy workflows (receive/dispense/return)
Cross-network interoperability (multiple blockchains or mixed tech stacks)
The FDA's exploration of blockchain interoperability concepts suggests that interoperability is an active area of experimentation, not a solved problem. U.S. Food and Drug Administration

8.3 Privacy, competition, and data ownership
Supply chains are competitive networks. Trading partners may resist sharing data that reveals volumes, routes, or relationships. Permissioned platforms help, but privacy-preserving analytics and selective disclosure remain challenging. Likely future directions include:
Policy-based encryption and key management aligned with roles
Private data collections and "need-to-know" channels
Auditable access logs to satisfy compliance audits
Research on privacy-preserving proofs for authenticity assertions (emerging)

8.4 IoT trust and the "oracle problem"
IoT devices are the oracles that connect physical reality to digital records. If devices are compromised, blockchain immutability preserves falsehoods permanently. Hence, research should emphasize:
Secure hardware provisioning and attestation
Sensor redundancy and anomaly detection
Cross-validation with logistics milestones (scan events vs GPS routes)
Human-in-the-loop quality release in high-stakes exceptions

8.5 Organizational adoption and cost
A recurring barrier is cost vs perceived benefit. Sensors, integration development, node hosting, and governance overhead can be significant, especially for smaller pharmacies. Adoption strategies that may improve feasibility:
Start with high-value/high-risk segments (cold-chain biologics, controlled substances)
Use shared service models (managed blockchain nodes, managed EPCIS repositories)
Provide incremental benefits (reduced chargebacks, faster receiving) before full transformation
Align incentives via consortium agreements and regulatory readiness programs

CONCLUSION

The pharmaceutical supply chain operates within one of the most highly regulated and risk-sensitive industrial environments, where failures in traceability, product integrity, or cold-chain compliance can directly affect patient safety and public health. This review has examined blockchain-enabled drug supply chain management (SCM) in pharmacy contexts, with a particular emphasis on its integration with Internet of Things (IoT) technologies and enterprise resource planning (ERP) systems. The synthesis demonstrates that blockchain's value does not lie in replacing existing enterprise infrastructure, but rather in acting as a shared trust and verification layer that enhances transparency, accountability, and coordination across organizational boundaries.

A key insight emerging from this review is that integration is the critical success factor. IoT devices provide real-time, physical-world evidence of drug handling conditions such as temperature, humidity, location, and tampering, which is especially vital for cold-chain pharmaceuticals and high-value biologics. However, IoT data alone lacks institutional trust when shared across multiple stakeholders. By anchoring cryptographic proofs and exception summaries on a permissioned blockchain, the integrity and non-repudiation of these physical events can be ensured without overwhelming the ledger with high-volume sensor data. This hybrid on-chain/off-chain approach offers a practical balance between scalability and auditability.

ERP systems remain central to pharmaceutical operations, governing inventory management, quality assurance, regulatory compliance, and financial reconciliation. The review highlights that blockchain-enabled SCM architectures are most effective when ERP systems retain their role as systems of record, while blockchain networks

function as systems of shared verification. Event-driven, asynchronous integration patterns allow ERP processes—such as goods receipt, authenticity verification, quarantine, release, and recall—to interact with blockchain networks without compromising enterprise performance or availability. This architectural separation reduces organizational resistance and aligns with existing regulatory expectations.

Interoperability is another dominant theme addressed in this paper. Standards such as GS1 EPCIS provide a common semantic foundation for representing supply chain events, enabling consistent interpretation across diverse partners. Blockchain networks that align with EPCIS-style event models—or that anchor off-chain EPCIS repositories—are better positioned to support regulatory frameworks such as the Drug Supply Chain Security Act (DSCSA), which emphasizes interoperable electronic tracing rather than specific technologies. The inclusion of interoperability gateways ensures that partial adoption does not fragment the ecosystem and allows gradual onboarding of pharmacies, distributors, and manufacturers.

Despite its promise, blockchain-enabled drug SCM faces persistent challenges. Scalability at serialization-level volumes, data privacy in competitive supply networks, governance of multi-stakeholder consortia, and the security of IoT "oracles" remain open research and implementation concerns. Smaller pharmacies may also face cost and capability barriers, underscoring the need for shared-service models and targeted deployment strategies focusing initially on high-risk or high-value product segments. Future research should prioritize large-scale empirical pilots, standardized conformance testing for traceability events, and privacy-preserving verification mechanisms that satisfy both regulators and commercial stakeholders.

In conclusion, blockchain-enabled drug supply chain management—when tightly integrated with IoT sensing and ERP-based execution—offers a compelling pathway toward more transparent, resilient, and trustworthy pharmaceutical distribution systems. Its true impact will be realized not through isolated pilots, but through standards-aligned, governance-backed, and economically sustainable deployments that address real operational and regulatory needs within pharmacy ecosystems.

REFERENCES

1. World Health Organization. Substandard and falsified medical products (Fact sheet, updated 3 Dec 2024). World Health Organization
2. World Health Organization. 1 in 10 medical products in developing countries is substandard or falsified (News release, 28 Nov 2017). World Health Organization
3. U.S. FDA. Drug Supply Chain Security Act (DSCSA) (updated 16 Oct 2025). U.S. Food and Drug Administration
4. U.S. FDA. DSCSA compliance policies establish 1-year stabilization period implementing electronic systems (30 Aug 2023). U.S. Food and Drug Administration
5. U.S. FDA. DSCSA Standards for the Interoperable Exchange of Information for Tracing… (Guidance, 5 Nov 2024). U.S. Food and Drug Administration
6. GS1. EPCIS Standard (EPCIS & CBV overview; EPCIS 2.0). GS1
7. Li, L., et al. (2022). A Blockchain-Based Product Traceability System with Off-chain EPCIS… Sensors, 22(22), 8680. MDPI
8. Sudha, C. M. N., et al. (2024). TrackChain: Hyperledger based pharmaceutical supply chain Heliyon. ScienceDirect
9. Mangala, N., et al. (2024). Secure pharmaceutical supply chain using blockchain in IoT-Cloud… Array. ScienceDirect
10. Duman, E., et al. (2025). Enhancing Traceability and Reliability in Cold Chain Logistics using Blockchain (Fabric) + IoT Applied Sciences. MDPI
11. U.S. FDA. Blockchain Interoperability Pilot Project Report (PDF). U.S. Food and Drug Administration
12. Abdallah, S., et al. (2023). Blockchain-based solution for Pharma Supply Chain Industry Computers in Industry. ScienceDirect
13. Grand View Research. Pharmaceutical cold chain packaging market size (2024 estimate; 2033 projection). Grand View Research
14. DataM Intelligence. Pharmaceutical cold chain logistics market size (2024; 2033 projection)
15. RamanathanT. T. (2025). DIFFERENTIAL PRIVACY AND HOMOMORPHIC ENCRYPTION–BASED PRIVACY-PRESERVING ENSEMBLE LEARNING FOR MEDICAL DIAGNOSIS. International Journal of Engineering Sciences & Research Technology, 14(12), 1–13. https://doi.org/10.29121/ijesrtp.v14.i12.2025.1
16. OKONJI K. S.(2025). ENVIRONMENTAL IMPACTS OF INDUSTRIAL ACTIVITIES ON SOIL AND WATER QUALITY: A COMPREHENSIVE REVIEW. International Journal of Engineering Sciences & Research Technology, 14(12), 14–25. https://doi.org/10.29121/ijesrtp.v14.i12.2025.2

