

Blockchain-Based Pharmaceutical Supply Chain Security for Counterfeit Drug Prevention

Aditya Sharma¹, Yatharth Yadav¹, Saksham Singh¹, Rohan

Kurup¹ G S Nagaraja², Sanjana Ravindra Otiha²

¹Dept. of CSE, R V College of Engineering, Bengaluru, India

²Professor, Dept. of CSE, R V College of Engineering Bengaluru, India

Abstract—The threat of counterfeit medicines to world health and public health in general is a constant and growing challenge, compromising patient safety and the trust of legitimate pharmaceutical products, supply chains. The current traceability systems, which are mainly based on centralised databases and systems, Paper-based record keeping is susceptible to falsification of records, insider manipulation of records, and other issues. There was a clear lack of transparency with stakeholders and a very basic lack of cross-stakeholder transparency. In this paper, a framework based on blockchain technology for end-to-end pharmaceutical supply-chain is proposed. Distributed ledger technology security that combines consortium distributed ledger technology and IoT enabled physical. smart contracts with cryptographically enforced enforce the conditions, and monitor for tampering activities. The provenances from manufacturer to patient. The framework is based on an architecture using a consortium permissioned approach with Practical Byzantine (PBFT) governance. Deterministic transaction finality is provided by Fault Tolerance (PBFT) consensus, which is bounded. Fault Tolerance (PBFT) consensus is bounded deterministic transaction finality, latency, and role-based access control for the regulatory requirements of pharmaceutical organizations. distribution. One of the on-chain/off-chain storage models with IPFS content-addressed storage Solve the conflict between scalability in data size and auditable blockchain use. A detailed security analysis covers the major attack vectors such as Sybil attacks, counterfeit injection, IoT spoofing, and smart contract vulnerabilities, and identifies Cryptographic and architectural countermeasures that correspond to the threats. The evaluation against representative previous architectures shows that The proposed framework delivers better throughput, lower latency, and access-control. preserves multi-party trust, with assurances that come with public-blockchain solutions. A set of properties that are missing in private blockchain deployments. The framework provides a replicable, standards-based structure for safe pharmaceutical supply chain. regulatory regimes such as traceability for modern-day needs the U.S. Drug Supply Chain Security Act and the EU Falsified Medicines Directive.

Index Terms—Blockchain, Counterfeit Medicines, Pharmaceutical Supply Chain, Smart Contracts, Internet of Things, Healthcare Security, Consortium Blockchain, Traceability, PBFT Consensus, IPFS, Distributed Ledger.

I. INTRODUCTION

Pharmaceutical counterfeiting is a serious issue in the global scenario. scale and consequence. The World Health Organization (WHO) estimates that up to 10Make up about 10countries. This crisis accounts for about 500,000 deaths that

could be prevented every year, The most reported falsified products are antibiotics and antimalarials. For example, it is estimated that in sub-Saharan Africa alone, 267,000 deaths are associated per year. to tampered antimalarial drugs and below-average drugs for childhood pneumonia. Can lead to 169,000 more deaths [1]. In addition to the immediate threat to patients, counterfeit medicines create significant economic loss. costs to manufacturers, costs to national health systems, and undermine trust in public health. health-care delivery. The total number of dollars lost due to pharmaceutical counterfeiting has been estimated at The problem has an annual global cost of USD 200 billion (USD 180 billion in the United States alone) and is growing more rapidly than we can imagine. However, conventional enforcement responses [2] remain.

These modern pharmaceutical supply chains involve several layers of actors such as manufacturers, primary or secondary distributors, logistics providers, wholesalers, retail and hospital pharmacies—and often cross international jurisdictions that have different regulatory frameworks for these drugs.pharmacies—and often times across international borders with different regulatory regimes for these drugs. requirements. Every scene change between characters presents a chance for a bogus switch-up, or adulteration. The industry's traditional central enterprise databases for recording custody transfers introduces systemic vulnerabilities: a single compromised or manipulated repository can corrupt provenance records throughout their whole distribution network without detection [23].

To elaborate, this supply chain faces a set of structural vulnerabilities that collectively enable the infiltration of counterfeit medicines. Paper-based batch pedigrees and even existing electronic serialisation schemes (such as the U.S. DSCSA and EU FMD) perform authentication only at discrete handoff checkpoints, leaving physical custody intervals unmonitored [3], [5]. Furthermore, fragmented inter-organisational data sharing makes cross-organisational verification cumbersome and technically unreliable [21]. When counterfeit products are identified, the absence of granular, real-time provenance records makes root-cause investigation and targeted recall difficult and slow [19].

To put it simply, there are a series of structural weaknesses in this supply chain all of which. allow for infiltration of

fake drugs. S. Food Aid systems are being updated to include paper-based batch pedigrees and even existing U.S. Food Aid systems. electronic serialisation schemes (including U.S. DSCSA and EU FMD) are used for authentication. In only discrete hand-off checkpoints, where there are no monitoring intervals of physical custody [3], [5]. In addition, there are data silos between organisations which means that data sharing is fragmented. There are technical and practical challenges with cross-organisational verification in the form of being cumbersome and unreliable abeyratne2016. When fake products are detected, the non-existence of granular real time provenance In records, recordings of the events of a specific project are kept separately from the evidence of the project's completion in order to facilitate a targeted recall, which makes it difficult and slow to investigate the cause of the failure or success of a project [19].

Particularly, distributed ledger technology (DLT), or blockchain, has garnered increased interest in recent years, as: These are limitations that are solved in a structural way by a new technology, namely the bitcoin protocol, the bitcoin network and the bitcoin blockchain, as described in [6], [7]. Smart contracts build on this foundation using business logic that is programmed and self-executing which enforces Rules in supply-chains without any trusted intermediary [10]. Although there has been a lot of research interest, there are significant architectural gaps. Public blockchains suffer from throughput problems and gas-cost barriers that. Preclude the volume of transactions needed for global unit-level serialisation zheng2018. What's more, full on-chain transparency means that commercially sensitive supply chain information becomes available to the public. competitors [20]. Private-blockchain architectures outperform them in terms of performance, Implement central operator control, which contradicts multi-party trust guarantees. There is no single, analytically grounded, and literature-based framework that co-designs The features include consortium blockchain governance, IoT physical monitoring, hybrid storage, and formal. security analysis. With the aim of creating a continuous traceability system, Justify a consortium architecture, propose smart contracts and modularize them, and create a hybrid storage system. model, and perform a proper security analysis, while taking regulatory needs into consideration. This paper attempts to fill in these gaps by making the following contributions:

- A four-layer blockchain-IoT framework for end-to-end pharmaceutical traceability, and Incorporating RFID, NFC and GPS sensing into consortium distributed ledger technology and smart-contract enforcement.
- A detailed comparison of the various types of blockchain architectures and consensus mechanisms. In response to pharmaceutical supply-chain requirements, mechanisms were developed to combat them, yielding a very good choice of consortium PBFT.
- A modular smart-contract architecture, spanning medicine registration, custody, and usage. immutable audit logging, transfer, expiry tracking.
- Hybrid approach to on-chain/off-chain storage with

content-addressed approach using IPFS”) A compromise has to be reached between auditability and scalability of operations in storage.

- A threat-model-driven security analysis along with mitigation, strategies Encompassing the major attack vectors of a distributed pharmaceutical ledger.

The scope of this work encompasses the comprehensive design, architectural justification, and formal security evaluation of an end-to-end traceability framework tailored specifically for the pharmaceutical sector. By proactively monitoring the physical transit intervals between discrete supply-chain checkpoints, this research bridges the critical gaps left by conventional electronic serialisation schemes. The significance of the proposed framework lies in its ability to successfully reconcile the stringent regulatory demands of patient safety and provenance tracking (such as the U.S. DSCSA and EU FMD) with the commercial necessities of data privacy and high transaction throughput. Ultimately, this scalable, tamper-resistant architecture provides a replicable foundation that not only curbs the infiltration of counterfeit medicines but also restores multi-party trust across global health-care delivery systems.

II. LITERATURE REVIEW

A. *Blockchain in Healthcare and Pharmaceutical Traceability*

The model of blockchain introduced by Nakamoto in [6] is the basic model. A peer-to-peer ledger architecture with attributes of decentralisation, cryptographic integrity and provenance. The and censorship resistance also generalised beyond the initial cryptocurrency. application. Buterin's Ethereum platform [7] improved upon this model by adding Turing-complete smart contracts, which allow for programmatic supply-chain logic without trusted intermediaries.

The first systematic study of blockchain's [10] [10] potential was carried out by Clauson et al. in an early study. Relevance for pharmaceutical supply chains, and concluding that immutable batch pedigrees were relevant. Could meet the requirements of the DSCSA for serialisation. Their analysis, however, was done mostly on the feasibility aspect and did not discuss consensus-mechanism Scalability architecture or selection. Sylim et al. [11] have developed a prototype on the Ethereum testnet and showed that What they noted was that smart contracts could be used to create automated mechanisms for custody enforcement and identify unauthorized transfers. attempts. The research stated that gas prices to the public blockchains are too high to make large-scale deployment possible. economically impractical.

Musamih et al. (2021) further broadened the design space to Hyperledger Fabric, and Enhance drug-batch lookup latency to < 1 second compared to public-Ethereum. baselines. Their system was designed to store metadata off-chain, using IPFS, but it didn't consider the formal There are two types of security model or consensus trade-off analysis. Kumar and Tripathi [15] added a suggestion to represent drug batches

by means of an ERC-721. The NFTs are hardened from batch splitting attacks, which is a method that enhances their security. anti-counterfeiting guarantee and is subject to the token-cost constraint of public Ethereum.

B. IoT Integration in Pharmaceutical Supply Chains

Kazutaka Shimizu's presentation on the use of IoT sensors for extending the traceability of pharmaceuticals into the physical world has been a recurring trend in the past few years. Jamil et al. [17] combined RFID tags with a private Ethereum chain for The data from blockchain is immutable and cold-chain monitoring, which was a hot topic, was proven. Temperature Sensitive biologics Records of environmental integrity. Fan et al. [18] suggested a unit level authentication based on on-chain QR code and NFC. Verification, which was found to be counterfeit-dispensing, was reduced when made available to the patient. Incidents that occur in a simulated retail pharmacy environment.

One of the first end-to-end use-cases, provided by Bocek et al., [19] has inspired us. Analysis of blockchain-based pharmaceutical cold-chain monitoring with hand-on discussion of the practical A couple of major hurdles facing the integration of Ethereum nodes and IoT gateways were the ability to combine the two in a scalable and secure manner, and the identification of data throughput as a key challenge. primary architectural bottleneck.

C. Scalability and Hybrid Storage

Applications like them have hampered its widespread adoption. The scalability issue of blockchain in these kinds of storage-intensive applications has impeded its mass use. The contexts of supply-chains are documented. Wood [16] established Mijarova found the storage requirements of full nodes are unlimited. As the chain gets longer the luminosity decreases. Shrestha and Vassileva [14] suggested Hybrid (HyF) channels that integrate IPFS with Hyperledger Fabric. storage for large medical records, with only the necessary ones retained. content-addressed hashes on-chain. This strategy is consistent. The concept is taken up and expanded upon in the current framework. Abeyratne and Monfared [23] talked about the general concept Of blockchain-ready supply chains, and hybrid on-chain and off-chain systems, he noted. As for the future, the chain/off-chain models would seem to be practically the only way to achieve high-frequency trades. volume industrial deployments

D. Consortium Blockchain and Consensus Mechanisms

Androulaki et al. [17] presented the Hyperledger Fabric Core (HFC) project, which utilizes both two public keys. ric's PBFT-based ordering service can attain throughputs more than 3,500 transactions per second (TPS)—an order of Under controlled network is the magnitude of public Ethereum. the digital sector. forming the basis for the viability of the consortium blockchain in the digital sector. enterprise supply chains. Zheng et al. [15] gave the following comprehensive analysis. The most comprehensive taxonomy of consensus

mechanisms and their trade-offs with respect to throughput, fault tolerance, finality, and energy consumption, which leads to consensus- The remainder of the article features selection analyses performed in later stages of the pharmaceutical-blockchain. studies. Casino et al. [18] have carried out a systematic review. Over 200 blockchain applications are present in various industries, and this number is still growing, on healthcare and supply-chain deployments, there is a disproportionate investment. favour permissioned architectures for their regulatory compli- Better performance in terms of latency and performance.

E. Security in Pharmaceutical Blockchain Systems

Lin and Liao [19] described the main security The vulnerabilities of blockchain deployments, such as smart- Resistance to contract bugs, Sybil attack and 51 Ahmad et al. [13] have suggested zero-knowledge-proof enhanced Pharma supply chains to be tracked and enabled via smart contracts. sitive information. compliance verification without sharing commercially sensitive information. Despite the study not assessing performance, sitive data. overhead comprehensively. Benchoufi and Ravaud [24] discussed Integrity Assurance for Clinical Trials based on the blockchain is a new concept. data, a related field with the same roots is the pharmaceutical industry's. A related field, with the same roots, is data. Tight auditability and tamper resistance requirements

F. Analytical Summary and Research Gap

Table I synthesises representative prior work across key dimensions. The analysis reveals three persistent gaps: (i) the absence of a unified framework that co-designs consortium blockchain governance, IoT integration, and hybrid storage as complementary components; (ii) limited formal security analysis in pharmaceutical blockchain designs; and (iii) insufficient comparative treatment of consensus mechanisms against pharmaceutical-specific performance and compliance requirements. The proposed framework addresses all three gaps.

III. PROPOSED FRAMEWORK

A. Overview

The proposed framework is structured across four vertically integrated layers, illustrated in Fig. 1. Each layer is functionally autonomous and communicates with adjacent layers through standardised interfaces, supporting incremental deployment and component-level upgrades without systemic disruption.

The supply-chain workflow enabled by the framework is depicted in Fig. 2.

B. Layer 1: IoT Data Acquisition

The data-acquisition layer constitutes the physical sensing infrastructure that translates real-world pharmaceutical events into digitally verifiable, blockchain-ready signals. Four sensing modalities are employed.

TABLE I
COMPARATIVE SUMMARY OF RELATED WORK

Author(s)	Technique	Blockchain Type	Advantages	Limitations
Clauson et al. [10]	Static batch pedigrees on Ethereum	Public	Immutable records; DSCSA alignment	High gas cost; no real-time monitoring
Sylim et al. [11]	Smart-contract custody enforcement	Public (Ethereum)	Automated transfer validation	Scalability; public data exposure
Musamih et al. [14]	Hyperledger + IPFS	Permissioned	Low latency; off-chain metadata	No formal security model
Kumar & Tripathi [15]	ERC-721 NFT drug tokens	Public	Batch-splitting prevention	Token cost; public-chain throughput
Jamil et al. [17]	RFID cold-chain + private Ethereum	Private	Environmental integrity records	Closed trust model; limited transparency
Fan et al. [18]	NFC + QR on-chain verification	Private	Consumer-facing authentication	Limited actor coverage; no RBAC
Ahmad et al. [25]	ZKP-enhanced smart contracts	Consortium	Privacy-preserving compliance	Performance overhead not evaluated
Bocek et al. [19]	IoT cold-chain gateway + Ethereum	Public	End-to-end cold-chain analysis	Throughput bottleneck identified
Proposed	Consortium BC + IoT + Hybrid Storage	Consortium (PBFT)	Unified framework; formal security analysis	Theoretical; awaits empirical validation

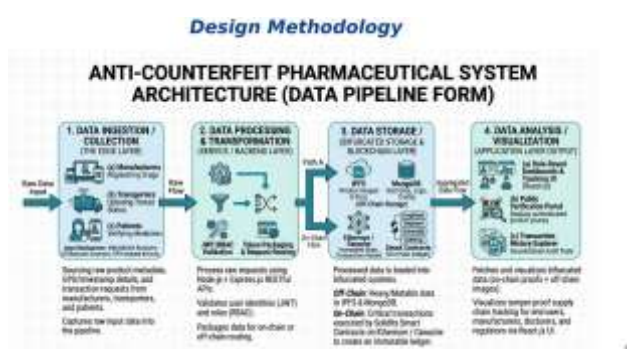


Fig. 1. Layered architecture of the proposed blockchain-IoT pharmaceutical supply-chain framework.

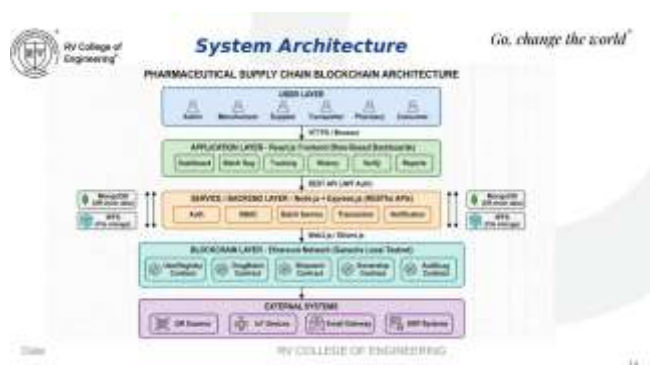


Fig. 2. End-to-end pharmaceutical supply-chain blockchain architecture.

RFID and NFC Tagging. Each drug unit or batch is affixed with a passive RFID or NFC tag carrying a globally unique identifier. Tag reads at designated checkpoints—manufacturing exit, distributor intake, cold-storage entry and exit, pharmacy intake—generate custody-transfer events that are cryptographically signed by the reading device and forwarded to the edge gateway. Passive RFID infrastructure is cost-effective at scale and compatible with existing pharmaceutical serialisation workflows.

GPS Location Monitoring. Active GPS tracking units attached to shipment containers transmit geolocation coordinates at configurable intervals throughout transit. Recorded locations are hashed and submitted to the blockchain, creating a tamper-evident position log. Route deviations beyond predefined geofence boundaries are flagged and escalated to the monitoring layer for regulatory notification.

Environmental Sensors. Temperature, humidity, and light-exposure sensors embedded within shipment containers provide continuous cold-chain integrity records. Sensor readings are timestamped locally, signed with the device's hardware-embedded key, and forwarded to the edge gateway. For temperature-sensitive biologics, excursion events constitute grounds for automatic batch-integrity flagging at the blockchain layer.

QR-Code Verification Interface. Each drug package carries a cryptographically secured QR code encoding the batch identifier and a digital signature over the unit's on-chain record. Pharmacists and, optionally, patients can scan the QR code to verify authenticity against the blockchain registry without requiring direct blockchain access, via a lightweight verification API.

C. Layer 2: IoT Monitoring and Edge Gateway

Edge processing nodes deployed at each supply-chain location aggregate raw sensor streams, apply local format nor-

malisation, and sign data payloads before submission to the blockchain layer. Processing at the edge reduces bandwidth overhead, minimises the latency between physical event occurrence and blockchain record creation, and enables pre-submission integrity checks that reject malformed or out-of-range sensor readings before they consume on-chain resources. A standardised pharmaceutical sensor data schema governs the format of all IoT-sourced submissions, enabling cross-manufacturer and cross-distributor data integration without custom adapter development.

D. Layer 3: Consortium Blockchain and Smart Contracts

The blockchain layer provides the immutable, distributed ledger infrastructure underpinning the framework. Its principal sub-components are described below; the smart-contract architecture is detailed further in Section IV, and the transaction workflow is depicted in Fig. 3.

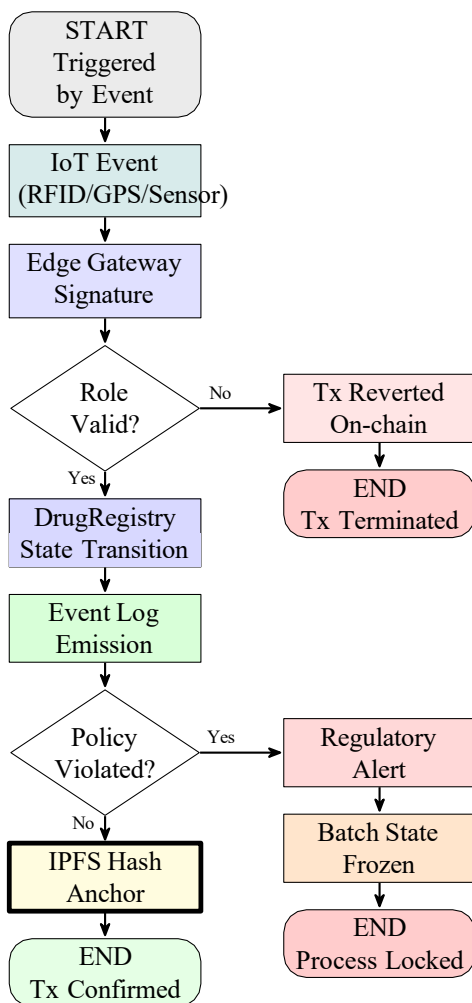


Fig. 3. Blockchain transaction workflow for a custody-transfer event, including termination points for all outcomes.

Distributed Ledger Infrastructure. A Hyperledger Fabric consortium chain is proposed as the ledger substrate, providing a channel-based permissioning model that allows bilateral or

multilateral data-sharing scopes to be configured independently of the global chain state [9].

Identity and Membership Management. A Membership Service Provider (MSP) maintains the public-key infrastructure for all consortium participants. Only entities with valid MSP certificates may submit transactions; anonymous or pseudonymous participation is not permitted, establishing a known-membership topology that is a prerequisite for PBFT consensus.

Smart Contract Layer. Chaincode (Hyperledger Fabric's smart-contract equivalent) encodes the business logic for drug registration, custody transfer, environmental compliance verification, and expiry monitoring.

Event Audit Log. All state-changing transactions emit structured events to the blockchain event log, providing a chronologically ordered, cryptographically verifiable provenance record accessible to authorised regulators without requiring full state replay.

E. Layer 4: Application and Stakeholder Interfaces

The application layer delivers role-differentiated user interfaces to each stakeholder class. Manufacturer portals support drug-batch registration and production record submission. Distributor and logistics interfaces manage custody-transfer workflows with real-time IoT-event overlays. Regulatory portals provide chain-wide audit views and configurable compliance dashboards. A lightweight consumer-verification interface—accessible via smartphone QR-code scan without requiring blockchain familiarity—provides binary drug-authenticity confirmation validated against the on-chain registry.

F. Consortium Blockchain Architecture Analysis

Three blockchain architecture paradigms are evaluated against the requirements of pharmaceutical supply chains. Table II presents a structured comparison, and Fig. 4 illustrates the consortium topology.

TABLE II
BLOCKCHAIN ARCHITECTURE COMPARISON FOR PHARMACEUTICAL APPLICATIONS

Criterion	Public	Private	Consortium
Decentralisation	High	Low	Medium
Throughput (TPS)	Low	High	High
Transaction Cost	High	None	Low
Participant Vetting	None	Full	Selective
Regulatory Fit	Poor	Medium	High
Data Confidentiality	Low	High	Configurable
Auditability	Full	Limited	Selective
Fault Tolerance	PoW/PoS	Owner	BFT-grade
Finality Type	Probabilistic	Instant	Deterministic
Suitability	Low	Medium	High

Public Blockchain is unsuitable for pharmaceutical applications for four reasons. First, the transaction throughput of Ethereum (approximately 15–20 TPS under practical conditions) is insufficient for the unit-level serialisation volumes of

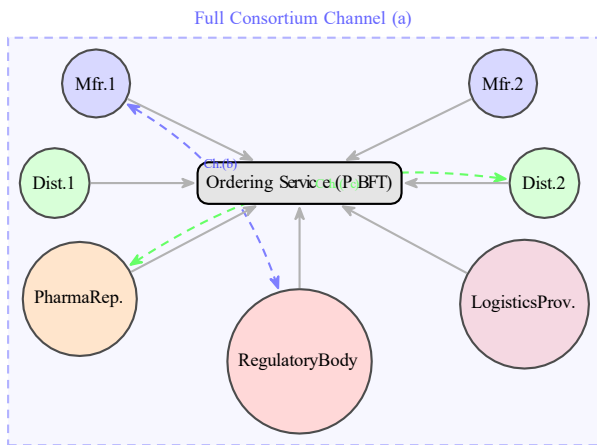


Fig. 4. Consortium blockchain network topology for pharmaceutical supply-chain governance.

a national pharmaceutical network. Second, gas fees introduce an economically unsustainable per-transaction cost for high-frequency IoT telemetry submissions. Third, the absence of participant vetting enables anonymous and potentially adversarial nodes to join the network, which is incompatible with regulated pharmaceutical distribution. Fourth, the full public visibility of on-chain data exposes commercially sensitive supply-chain information to competitors [10], [22].

Private Blockchain addresses throughput and privacy concerns but reintroduces the centralisation risks that motivate blockchain adoption. A single controlling organisation can alter, censor, or selectively disclose ledger records, meaning that competing supply-chain actors have no independent verification guarantee. The resulting trust model is structurally equivalent to a conventional centralised database [23].

Consortium Blockchain provides the optimal balance for pharmaceutical supply chains. Membership is restricted to vetted, known organisations—manufacturers, distributors, logistics providers, and regulatory bodies—eliminating anonymous participation while preserving independent multi-party verification. Governance is distributed among accountable consortium members under a formal governance agreement, preventing any single actor from unilaterally altering records. PBFT-class consensus provides deterministic transaction finality, satisfying the batch-recall workflows that require immediate, irreversible state updates. Channel-based data partitioning allows commercially sensitive bilateral data to be scoped appropriately without affecting chain-wide visibility [9].

G. Consensus Mechanism Analysis

Table III compares four consensus mechanisms across dimensions relevant to pharmaceutical supply-chain deployments.

Proof of Work (PoW), the consensus mechanism of Bitcoin and early Ethereum, is categorically unsuitable. Its computational intensity yields throughputs far below pharmaceutical requirements, probabilistic finality is incompatible with time-sensitive batch-recall operations, and its energy consumption

TABLE III
CONSENSUS MECHANISM COMPARISON FOR PHARMACEUTICAL SUPPLY CHAINS

Criterion	PoW	PoS	PBFT	PoA
Throughput (TPS)	<20	<100	>1000	>500
Confirmation Latency	High	Medium	Low	Low
Energy Consumption	High	Low	Low	Low
Finality Type	Prob.	Prob.	Deter.	Deter.
BFT Guarantee	51%	33%	33%	Identity
Permissioning	None	None	Native	Native
Governance Fit	Poor	Medium	High	High
Pharmaceutical Suitability	Poor	Low	High	Medium

profile is ecologically untenable for enterprise deployment [6], [22].

Proof of Stake (PoS) improves upon PoW in energy efficiency and, in some implementations, throughput. However, it retains probabilistic finality and lacks native participant permissioning, rendering it unsuitable as the primary consensus mechanism for a regulated, known-membership consortium chain.

Practical Byzantine Fault Tolerance (PBFT) is recommended as the consensus mechanism for the proposed framework. PBFT achieves deterministic transaction finality within three communication rounds, guarantees correct operation in networks with up to f Byzantine-faulty nodes among $3f+1$ total validators, and is natively integrated with Hyperledger Fabric's ordering service [9]. Its throughput in well-parameterised deployments exceeds 1,000 TPS, sufficient for the peak transaction demands of a national pharmaceutical supply chain. The primary constraint of PBFT—quadratic message complexity $O(n^2)$ —limits practical consortium size to approximately 100 validators, which is sufficient for pharmaceutical industry deployments but requires hierarchical PBFT variants for global multi-jurisdiction consortia.

Proof of Authority (PoA) provides a simpler, lightweight alternative for smaller consortia where validator identity serves as the sole Sybil-resistance mechanism. Its lower communication overhead makes it attractive for resource-constrained deployments, though it provides weaker Byzantine fault tolerance guarantees than PBFT.

IV. SMART CONTRACT ARCHITECTURE

The smart-contract layer applies business logic of the supply-chain in a hierarchy of smart-contracts. Well-defined functional scope interacting contracts. The design principle of separation of concerns was used to allow for a more independent design. Component-level upgrades and auditing. **AccessControl Contract.** Provides the authoritative list of participants' roles: MANUFACTURER, The groups are: DISTRIBUTOR, LOGISTICS, PHARMACY and REGULATOR. Role assignments are only controlled by the Regulatory Authority

node and propagated via the consortium's MSP. All state-changing functions in downstream contracts have role validation guards on each of them. revert unauthorised calls on-chain, so that no actor can perform outside operations their designated scope.

DrugRegistry Contract. Sustains the "canonical" record of each pharmaceutical batch. A replica of the global batch identifier and the manufacturer's identifier for the manufacturer that registered the record are included in each record. The address, manufacturing and expiry timestamps, the current custodian, a state enum reflecting the position of the batch in the supply chain, as well as an IPFS content identifier for off-chain metadata, and an environmental-integrity flag maintained through the submission of events through IoT. A deterministic finite-state machine is used to enforce custody-state transfers: If an attempt to make a transition in the wrong sequence is attempted, it will undo the transaction on-chain, and thus the transaction will fail. Falsified records as manipulated custody-state records.

TransferControl Contract. Shares custody between role adjacent actors. Transfers must be confirmed by both the relieving and relieving party, It is meant to be a cryptographic log of mutual consent and prevent impersonation attacks.

AlertOracle Contract. Compares the incoming IoT telemetry with the policy rules set: Temperature excursion. Thresholds, geofence violation distances and expiry proximity window. Batch-state freezes are automatically generated by violations of policy and regulatory alert events are triggered, Avoiding the delay of manual workflows for inspections.

Audit Log. Every state transition results in a structured, indexed on-chain event. The event log is a cryptographically ordered and immutable audit trail that regulatory bodies can query for compliance verification without having to go through the full contract state.

V. HYBRID ON-CHAIN/OFF-CHAIN STORAGE MODEL

A. Scalability Limitations of Full On-Chain Storage

Collecting all pharmaceutical metadata, such as regulatory certificates, batch composition, etc. documents, environmental telemetry archives and photographic product records—completely on-chain is simply not feasible architecturally. Even Hyperledger Fabric's efficient leveldb state database couldn't help the high-frequency IoT applications. scale of telemetry ingestion would result in ledger growth rates that would be incompatible with the The cost of distributed validator nodes' storage [8].

B. IPFS-Based Off-Chain Storage

In the framework, the off-chain storage used is based on IPFS (InterPlanetary File System). substrate. Each data object is given a content identifier (CID) by IPFS based on the data object. cryptographic hash. As the CID is deterministically linked to the content, any change to an Each time a new document is created with off-chain document, the CID is different, resulting in the reference on-chain being different. become ineffective and the tampering be immediately apparent. This

property guarantees integrity similar to on-chain storage of this property. The metadata objects themselves, without taking up the bulk on the ledger.

C. Storage Architecture and Tiering

On-chain records are limited to: the batch CID, a hash of the corresponding batch (SHA-256). Can be stored on IPFS: document, state enum, minimal indexable metadata (batch ID, expiry timestamp, current custodian). This limits the amount of data stored on-chain per drug record to about 256 bytes.

Data of all the batches is stored on chain, as is complete regulatory information; Off-chain IPFS stores: complete regulatory documentation, batch composition and Quality assurance certificates, environmental telemetry archives, and chain of custody. photographic records. The edges use an edge-cloud tiering model that manages retention - high-frequency raw IoT streams are retained. Archival to IPFS, while on-chain is a temporary option that requires the archive service to be run at edge nodes for a user-defined short-term period before it can be archived. The references for CID will not be removed from the chain for the life of the chain.

The hybrid architecture is illustrated in Fig. 5.

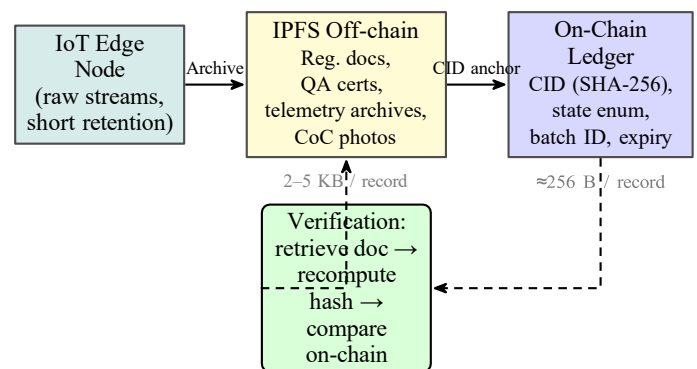


Fig. 5. Hybrid on-chain/off-chain storage architecture with IPFS content-addressing.

D. Storage Efficiency

A total of approximately 256 bytes of on-chain storage is used per drug unit, in contrast to an. If the full off-chain metadata is estimated to be 2-5 KB, then the storage-efficiency ratio is. The on-chain designs are approximately 15x bigger than full designs. This increases the life of the consortium chain in use and decreases The following features will be provided by the system to help make participation easier: Smaller players in the supply-chain like regional distributors and independent pharmacies.

VI. SECURITY ANALYSIS

A. Threat Model

The threat model covers six categories of attacks across the framework's principal surfaces, spanning the IoT acquisition layer (RFID/NFC cloning, sensor spoofing, MITM), the edge gateway layer (device key compromise, firmware

manipulation), the blockchain and smart-contract layer (Sybil, replay, smart-contract exploits, insider manipulation), and the application interface layer (access-control bypass, phishing).

B. Attack Vectors and Mitigations

Table IV enumerates the principal attack vectors, their assessed risk levels, and the corresponding mitigation strategies.

TABLE IV
SECURITY THREAT ANALYSIS AND MITIGATION STRATEGIES

Attack Vector	Risk	Mitigation
Sybil Attack	High	Consortium identity vetting; MSP PKI certificates; PBFT permissioned consensus
51% / Eclipse Attack	Medium	PBFT BFT guarantee; bounded known-membership topology
Replay Attack	High	Transaction nonces; timestamp validity windows; chain-ID binding
IoT Spoofing / MITM	High	TLS 1.3 device-to-gateway; HSM-backed device signing keys; gateway signature verification
Smart Contract Exploit	High	Audited contract libraries; checks-effects-interactions pattern; formal contract verification
Insider Manipulation	Medium	Dual-signature transfers; RBAC enforcement; immutable audit log; multi-signature approvals
Counterfeit Injection	Critical	Manufacturer HSM signing; dual-signature batch registration; on-chain duplicate-ID checks
IPFS Content Poisoning	Low	On-chain SHA-256 hash binding; IPFS pinning policy; CID mismatch detection

Role-Based Access Control (RBAC). The AccessControl contract enforces strict role separation, ensuring that each stakeholder can only execute the operations appropriate to their supply-chain function. RBAC is a well-established countermeasure against insider privilege escalation and accounts for the majority of access-related threat mitigations in the framework [26].

Cryptographic Hashing and Integrity. SHA-256 hashes anchor off-chain IPFS documents to on-chain records. All IoT-sourced events are cryptographically signed at the device level using hardware-embedded keys, preventing record injection by compromised or impersonated gateways.

Multi-Signature Verification. High-consequence operations—batch registration, recall initiation, and regulatory audit access—require m -of- n multi-signature approval from designated authorities. This ensures that no single actor, even one with legitimate credentials, can unilaterally execute critical state changes, providing resilience against compromised accounts.

Zero-Knowledge Proofs for Selective Compliance Verification. Following Ahmad et al. [25], the framework accommodates ZKP-based selective disclosure for sensitive pharmaceutical metadata. A supply-chain actor can demonstrate to a regulator that a batch satisfies a compliance condition—temperature remaining within bounds throughout transit—without revealing the underlying raw telemetry data to unauthorised parties.

VII. PERFORMANCE ANALYSIS

A. Throughput and Latency

Multiple vendors have achieved throughputs of 3,500+TPS for PBFT consensus on Hyperledger Fabric. In a well-parameterised network conditions, end-to-end transaction confirmation latencies below 300 ms [9]. This is significantly higher than the peak transaction demand that is estimated for a national pharmaceutical. concurrent unit-level serialisation events: 500 TPS in the distribution network. In all chain levels. The load on the blockchain-layer can be further reduced by about 30-40Local aggregation and early rejection of malformed sensor payloads.

B. Storage Overhead

The hybrid storage model reduces per unit costs as quantified in Section V. In addition, the on-chain storage is reduced by about 1/15 compared to Full on-chain. designs. At an estimated 256 bytes per on-chain record and a national pharmaceutical market processing 10 billion unit-level events per year, the annual on-chain ledger growth is limited to about 2.5 TB within the consortium, which is a reasonable amount of storage. For enterprise class validator nodes.

C. Comparative Evaluation

Table V presents a comparative performance summary against representative prior architectures.

D. Interoperability

Interoperability between the proposed consortium chain and legacy pharmaceutical ERP and warehouse management systems is achieved through RESTful API gateways that translate on-chain event data into industry-standard messaging formats (GS1 EPCIS, HL7 FHIR). Cross-chain interoperability with other national or regional pharmaceutical consortia can be addressed through relay-chain architectures or standardised cross-chain communication protocols in future iterations of the framework.

VIII. PRIVACY AND REGULATORY CONSIDERATIONS

A. Role-Based Transparency Model

The framework has a three-layered transparency model reflecting the roles of the stakeholders. Public data (drug serial numbers and dispensing confirmations) is available to As a consumer-verification interface, they will facilitate patients. Consortium-visible data – custody transfer records environmental telemetry All vetted members of the consortium

TABLE V
COMPARATIVE PERFORMANCE SUMMARY

System	Blockchain Type	Max TPS	Avg. Latency	Storage Model	Security Analysis
Clauson et al. [10]	Public Ethereum	~15	>10 s	On-chain only	Informal
Sylim et al. [11]	Public Ethereum	~20	8–12 s	On-chain only	Partial
Musamih et al. [14]	Hyperledger	~800	<1 s	On-chain + IPFS	Not formal
Ahmad et al. [25]	Consortium	~300	~2 s	On-chain only	ZKP-focused
Proposed	Consortium (PBFT)	>3,500	<300 ms	Hybrid (IPFS + Edge)	Formal threat model

have access to summaries—is. information—will not be disclosed. However, formulation information, pricing agreements and patient-specific data will not be made available, the latter being considered to be *Restricted* data. dispensing identifiers—is only available to parties directly involved and the Regulatory Enforced by Hyperledger Fabric’s channel-based data partitioning.

Data Minimisation and Pharmaceutical Privacy

At the patient-verification step no personal health data is saved on-chain. Only an anonymised transaction hash is created in the consumer-verification interaction, Complying with the data minimization principle under GDPR regulating data use. frameworks. Problems of blockchain immutability and data erasing rights are solved can be stored in IPFS documents off the blockchain and then retrieved on-demand. This has been achieved by removing IPFS pins so that the on chain CID reference is no longer resolvable. Without changing chain record.

B. Regulatory Alignment

The framework will meet the technical needs of the U.S. DSCSA— The 4 main features of unit-level serialisation are: transaction statements and the unique identifiers and other requirements of the EU FMD. In the context of tamper evident packaging, the packaging verification is crucial [3], [5]. The consortium has dedicated regulatory-authority nodes that have read-only access to the complete audit event log is available and real-time compliance monitoring can be done without needing to Having been involved in transaction ordering.

IX. CONCLUSION AND FUTURE WORK

The current study aims to propose a secure, blockchain-integrated model for the pharmaceutical supply chain aimed at combating the ever-prevailing problem of the proliferation of counterfeit medicines. The framework provides end-to-end tamper-proof traceability for all tiers of the supply chain and inter-node distance, as well as the physical monitoring gaps, which the existing serialisation schemes are unable to monitor. The comparative analysis of blockchain architecture types provides evidence that consortium permissioned blockchain architectures provide better throughput, data confidentiality, compliance and multi-party trust than both public and private blockchain architectures. The performance features that are suited for large national-scale pharmaceutical serialisation workloads have been selected for PBFT consensus and are

the basis for the selection. PBFT consensus has been chosen for its performance features: deterministic finality, BFT fault tolerance, and Hyperledger Fabric compatibility.

The smart-contract architecture provides programmatic and immutable enforcement of supply-chain business rules: automatic sequence of custody transfers, expiry management, automated policy alerting, etc., without the need for trusted intermediaries and without the delay of manual verification among existing deployments. The hybrid IPFS-based storage model further expands the use of the model’s practical scalability to high-frequency IoT telemetry volumes without compromising the cryptographic integrity guarantees that are a core part of the anti-counterfeiting value proposition of blockchain.

The formal security analysis shows that the proposed system is resistant against the main attack techniques that pose threats to pharmaceutical blockchain systems, which include mitigative measures such as cryptographic hardware security, role-based access control, multi-signature governance, and selectively disclosure via zero-knowledge-proofs. The proposed framework represents a step towards implementing a standards-based, interoperable and economically viable traceability framework that directly contributes to the goals of UN SDG 3 (Good Health and Well-being) and is part of the larger agenda of transparent, accountable healthcare supply-chain governance.

Going forward, further research is planned to explore scalable BFT consensus mechanisms such as HotStuff for wide-ranging deployments and the use of cutting-edge zero-knowledge proofs (zk-SNARKs and zk-STARKs) to ensure privacy-preserving regulatory audits. In addition, we are working to bring the lightest possible verification logic at the IoT edge to perform real-time screening and investigate NFTs for drug identities to prevent batch splitting. This framework can eventually be interconnected with larger, decentralized healthcare systems that include clinical trials and patient data management by empirical pilot deployments and working with standardisation bodies (GS1, ISO, IEEE).

REFERENCES

- [1] World Health Organization, *Substandard and Falsified Medical Products*, WHO, Geneva, Switzerland, Fact Sheet, 2023. [Online]. Available: <https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products>

- [2] INTERPOL, "Operation Pangea XIII: Global results," INTERPOL, Lyon, France, Technical Report, 2020. [Online]. Available: <https://www.interpol.int/News-and-Events/News/2020/>
- [3] U.S. Food and Drug Administration, "Drug Supply Chain Security Act (DSCSA)," FDA, Silver Spring, MD, 2023. [Online]. Available: <https://www.fda.gov/drugs/drug-supply-chain-security-act-dscsa>
- [4] European Medicines Agency, "Falsified medicines: Overview and regulatory framework," EMA, Amsterdam, The Netherlands, 2023. [Online]. Available: <https://www.ema.europa.eu/en/human-regulatory/overview/public-health-threats/falsified-medicines>
- [5] European Commission, "Commission Delegated Regulation (EU) 2016/161 supplementing Directive 2001/83/EC on safety features appearing on the packaging of medicinal products for human use," *Official Journal of the European Union*, L 32, pp. 1–27, Feb. 2019. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0161>
- [6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Bitcoin.org*, Oct. 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [7] V. Buterin, "A next-generation smart contract and decentralised application platform," *Ethereum White Paper*, Ethereum Foundation, 2014. [Online]. Available: <https://ethereum.org/en/whitepaper/>
- [8] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Yellow Paper*, Ethereum Foundation, Apr. 2014, rev. 2022. [Online]. Available: <https://ethereum.github.io/yellowpaper/paper.pdf>
- [9] E. Androulaki *et al.*, "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proc. ACM EuroSys*, Porto, Portugal, Apr. 2018, Art. no. 30, doi: 10.1145/3190508.3190538.
- [10] K. A. Clauson, E. A. Breeden, C. Davidson, and T. K. Mackey, "Leveraging blockchain technology to enhance supply chain management in healthcare: An executive perspective," *Blockchain in Healthcare Today*, vol. 1, pp. 1–12, May 2018, doi: 10.30953/bhty.v1.20.
- [11] P. Syllim, F. Liu, A. Marcelo, and P. Fontelo, "Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention," *JMIR Research Protocols*, vol. 8, no. 9, p. e13395, Sep. 2019, doi: 10.2196/13395.
- [12] M. Mamoon and I. Shah, "A pharmaceutical supply chain management using blockchain and IoT," in *Proc. Global Conf. Information Technologies and Communications (GCITC)*, Dec. 2023, pp. 1–5, doi: 10.1109/gcitic60406.2023.10426356.
- [13] A. Nimsadkar and A. Pethe, "Blockchain in pharmaceutical supply chain management," in *Proc. 2nd DMIHER Int. Conf. Artificial Intelligence in Healthcare, Education and Industry (IDICAIEI)*, Nov. 2024, pp. 1–6, doi: 10.1109/idicaiei61867.2024.10842777.
- [14] A. Musamih, K. Salah, R. Jayaraman, J. Arshad, M. Debe, Y. Al-Hammadi, and S. Ellahham, "A blockchain-based approach for drug traceability in healthcare supply chain," *IEEE Access*, vol. 9, pp. 9525–9543, Jan. 2021, doi: 10.1109/ACCESS.2021.3049920.
- [15] A. Kumar and R. Tripathi, "A blockchain-based pharmaceutical supply chain using non-fungible tokens," *Journal of Medical Systems*, vol. 45, Art. no. 84, Aug. 2021, doi: 10.1007/s10916-021-01752-1.
- [16] L. Wang, Z. He, and D. Wu, "Design of a blockchain-enabled traceability system for counterfeit drug prevention," *Expert Systems with Applications*, vol. 213, Art. no. 118942, Mar. 2023, doi: 10.1016/j.eswa.2022.118942.
- [17] F. Jamil, S. Ahmad, N. Iqbal, and D.-H. Kim, "Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals," *Sensors*, vol. 20, no. 8, Art. no. 2195, Apr. 2020, doi: 10.3390/s20082195.
- [18] W. Fan, S. Chang, J. Wang, O. Alzahrani, and W. Li, "A novel NFC and blockchain-based pharmaceutical product authentication and anti-counterfeiting system," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Rhodes Island, Greece, Nov. 2020, pp. 478–483, doi: 10.1109/Blockchain50366.2020.00069.
- [19] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere — a use-case of blockchains in the pharma supply-chain," in *Proc. IFIP/IEEE Symp. Integrated Network and Service Management (IM)*, Lisbon, Portugal, May 2017, pp. 772–777, doi: 10.23919/INM.2017.7987376.
- [20] A. K. Shrestha and J. Vassileva, "User data sharing frameworks: A blockchain-based incentive solution," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Halifax, NS, Canada, 2020, pp. 295–302, doi: 10.1109/Blockchain50366.2020.00044.
- [21] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *International Journal of Research in Engineering and Technology*, vol. 5, no. 9, pp. 1–10, Sep. 2016.
- [22] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018, doi: 10.1504/IJWGS.2018.095647.
- [23] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telematics and Informatics*, vol. 36, pp. 55–81, Mar. 2019, doi: 10.1016/j.tele.2018.11.006.
- [24] M. Kumar, S. Chand, and C. P. Katti, "A secure and efficient blockchain-based healthcare data management system using IPFS," *IEEE Internet of Things Journal*, vol. 9, no. 19, pp. 18776–18788, Oct. 2022, doi: 10.1109/IJOT.2022.3162355.
- [25] A. Ahmad, M. Saad, and D. Mohaisen, "Secure and transparent pharmaceutical supply chain using permissioned blockchain with zero-knowledge proofs," *IEEE Transactions on Engineering Management*, vol. 68, no. 5, pp. 1411–1423, Oct. 2021, doi: 10.1109/TEM.2021.3069494.
- [26] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," *International Journal of Network Security*, vol. 19, no. 5, pp. 653–659, Sep. 2017, doi: 10.6633/IJNS.201709.19(5).01.
- [27] M. R. Islam and M. M. Rashid, "A survey on blockchain security and its impact analysis," in *Proc. 9th Int. Conf. Computer and Communication Engineering (ICCE)*, Aug. 2023, pp. 1–6, doi: 10.1109/icce58854.2023.10246031.
- [28] M. A. Rouzbahani and H. G. Garakani, "Blockchain security threats: Survey," in *Proc. 11th Int. Symp. Telecommunications (IST)*, Oct. 2024, pp. 171–175, doi: 10.1109/ist64061.2024.10843593.
- [29] M. Pandita *et al.*, "A survey on security attacks on blockchain using deep learning," in *Proc. IEEE Int. Conf. Blockchain and Distributed Systems Security (ICBDS)*, Oct. 2023, pp. 1–5, doi: 10.1109/icbds58040.2023.10346307.
- [30] A. Shahzad, L. Qiao, C. Wenyu, and A. Narejo, "Blockchain-based patient-to-individual secure medical data sharing," in *Proc. 21st Int. Comput. Conf. Wavelet Active Media Technology and Information Processing (ICCWAMTIP)*, Dec. 2024, pp. 1–7, doi: 10.1109/ic-cwamtip64812.2024.10873704.
- [31] Y. Li *et al.*, "Research on blockchain-based access control technology for medical data," in *Proc. 4th Int. Conf. Blockchain Technology and Information Security (ICBTIS)*, Aug. 2024, pp. 18–24, doi: 10.1109/icbtis64495.2024.00011.
- [32] Y. Li, G. Zhang, B. Feng, and S. Yang, "A medical data sharing scheme based on blockchain attribute-based searchable encryption," in *Proc. 4th Int. Conf. Computer Science and Blockchain (CCSB)*, Sep. 2024, pp. 539–542, doi: 10.1109/ccsb63463.2024.10735678.
- [33] Y. Chen, X. Li, and S. Wang, "Blockchain-based electronic health record access control scheme with secure and efficient sharing," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 8, pp. 3789–3798, Aug. 2022, doi: 10.1109/JBHI.2022.3168249.
- [34] A. A. Dar, F. A. Reegu, S. Ahmed, and G. Hussain, "Blockchain technology and artificial intelligence based integrated framework for sustainable supply chain management system," in *Proc. 11th Int. Conf. Computing for Sustainable Global Development (INDIACom)*, Feb. 2024, pp. 1392–1397, doi: 10.23919/indiacom61295.2024.10498149.