DOI: https://doi.org/10.61762/pjstvol8iss2art003

PLATFORM - A Journal of Science & Technology

Received: 22 October 2025, Revised: 18 November 2025, Accepted: 26 November 2025, Published: 31 December 2025, Publisher: UTP Press, Creative Commons: CC BY 4.0

# BLOCKCHAIN–IOT–IPFS FRAMEWORK FOR SECURE LOGISTICS TRACEABILITY

**Yahaya Saidu[1,2]*, Shuhaida Mohamed Shuhidan[1], Izzatdin Abdul Aziz[1]**

[1]Department of Computing, Universiti Teknologi PETRONAS, Malaysia
[2]Department of Computer Science, Taraba State University, Nigeria

Corresponding author: saidu_22009803@utp.edu.my

## ABSTRACT

*The growing demand for transparency and trust in logistics has exposed the limitations of centralised traceability systems, particularly in high-stakes sectors such as Halal trade, pharmaceuticals, and agri-food. This paper presents a decentralised framework that integrates blockchain (BC), Internet of Things (IoT), and the Interplanetary File System (IPFS) to support secure, real-time, and scalable logistics traceability. The proposed framework utilises Hyperledger Fabric, a permissioned blockchain, to ensure tamper-proof recording of logistics events and verifiable access control among stakeholders. IoT devices enable the continuous sensing of critical parameters such as temperature, location, and handling conditions, while IPFS supports off-chain storage of large sensor payloads with verifiable hash linking. Implementation involved setting up a Hyperledger Fabric v2.5 network, configuring Certificate Authorities, creating channels, deploying smart contracts, and integrating sensor data sources for real-time event capture. Performance evaluation was conducted using Hyperledger Calliper under both read- and write-intensive workloads. Results show that the system achieved up to 600 transactions per second (TPS) for read operations and 130 TPS for write operations, with sub-second latency and a near 100% transaction success rate under optimal load conditions. Offloading payloads to IPFS reduced on-chain storage by over 60%, preserving auditability without compromising performance. Compared to traditional centralised systems, the proposed framework demonstrates superior scalability, integrity, and operational readiness for real-world logistics applications, especially in compliance-sensitive and SME-driven environments.*

***Keywords:*** *Compliance enforcement, decentralised systems, hala logistics, off-chain storage, shipment monitoring, smart contracts, supply chain transparency, tamper-proof records*

## INTRODUCTION

In many supply chain systems today, tracking the movement and condition of goods, particularly in sensitive domains like pharmaceuticals or frozen food, is easier said than done. What happens when a vaccine shipment crosses borders, passing through multiple handlers and storage environments? Who ensures the data remains untampered, accurate, and verifiable in real time? These are not just operational concerns; they speak directly to public health, trust, and compliance [1]. Traditional logistics traceability systems are often built around centralised architectures. While this may seem practical at first, such systems are prone to well-known pitfalls, including fragmented data silos, the risk of tampering, and single points of failure [2]. Imagine a cold chain distribution network in which temperature sensors record a breach, but the data is either delayed or manipulated before reaching stakeholders. In high-compliance industries, this delay can result in product spoilage, financial losses, or even risk to lives [3].

This study proposes a new approach that combines the strengths of blockchain (BC), the Internet of Things (IoT), and the Interplanetary File System (IPFS) to form a decentralised framework for secure and scalable logistics traceability. Each of these technologies plays a specific role. BC ensures that once a shipment event is recorded, it cannot be altered without detection [4]. IoT devices offer real-time environmental sensing capabilities, including temperature, location, and humidity [5]. IPFS addresses one of the most pressing

issues in BC deployments: how to store large, high-frequency sensor data without overwhelming the network [6]. Through its modular design, the framework facilitates trustworthy data exchange among logistics partners while delivering strong performance across key metrics, including latency, throughput, and security. More than just a theoretical concept, the system has been prototyped using Hyperledger Fabric (HLF) and IPFS, tested with realistic logistics scenarios, and benchmarked against industry-relevant metrics. In doing so, it points toward a future where supply chain transparency is not just a goal, it is the default.

**Blockchain for Trusted Validation**

Beyond its role as a decentralised ledger, the architectural design of blockchain platforms, particularly their consensus mechanisms and permission models, plays a pivotal role in determining suitability for logistics applications. In multi-stakeholder environments where data integrity, performance, and privacy coexist as critical concerns, the choice of blockchain protocol becomes highly consequential.

Public blockchains such as Ethereum rely on consensus models like proof of work (PoW) or proof of stake (PoS), which prioritise openness and immutability but often introduce scalability bottlenecks, transaction delays, and limited control over data visibility [7]. These characteristics pose challenges for logistics operations that require fast processing, controlled disclosure, and policy-driven data segmentation.

In contrast, permissioned blockchains like HLF employ more efficient consensus mechanisms, such as RAFT and Practical Byzantine Fault Tolerance (PBFT). These protocols offer faster transaction finality and higher throughput by limiting consensus participation to known, authorised entities [8]. More importantly, HLF supports private data collections, channel isolation, and membership service providers (MSPs) for identity-based access, allowing stakeholders to interact within clearly defined trust boundaries [9]-[12].

This controlled environment also enhances the blockchain's utility for fraud detection, particularly in preventing actions like data tampering, false delivery confirmations, or unauthorised status overrides. When combined with smart contract logic, blockchain can autonomously flag suspicious events and enforce pre-defined corrective actions, thus reinforcing compliance and accountability within the supply chain [13].

**IoT for Real-Time Monitoring**

The IoT serves as the frontline for capturing logistics data, utilising devices such as GPS trackers, RFID tags, and temperature sensors to monitor goods across transportation nodes [14]. These sensors generate continuous, real-time data on shipment status, location, and environmental conditions. A typical IoT stack includes layers for sensing, communication, processing, and application delivery. However, without trusted infrastructure, sensor data remains susceptible to spoofing, loss, or unauthorised modification, posing risks to traceability accuracy, particularly in shared or cross-border supply chains [5].

**IPFS for Decentralised Off-Chain Storage**

BC's immutability comes at a cost: limited storage capacity and high transaction fees. To address this, the framework integrates the IPFS, which enables decentralised, content-addressed storage of large data objects. Files are split into chunks, hashed, and distributed across a peer-to-peer network. The resulting hashes are immutable and can be recorded on-chain to ensure verifiability. This design enables logistics systems to store high-frequency sensor data, compliance records, or images off-chain, thereby preserving blockchain efficiency while maintaining data integrity [15].

**Synergistic Integration of Blockchain, IoT and IPFS**

Individually, each component in this triad contributes a vital layer to logistics traceability: IoT offers real-time sensing and environmental monitoring; blockchain ensures verifiable, tamper-evident logging; and IPFS provides scalable, decentralised storage for high-volume data. When integrated, they form a cohesive and resilient traceability infrastructure that overcomes the limitations of centralised or siloed systems.

The synergy between these components lies in their complementary roles. For example, during cold chain transportation, if a temperature breach is detected by IoT sensors, a smart contract can be triggered to automatically log the violation on the blockchain, ensuring transparency and immutability. Simultaneously, the associated sensor logs and metadata are stored in IPFS, and the corresponding

hash is linked on-chain. This dual-layer approach not only reduces blockchain bloat but also guarantees that data remains auditable, retrievable, and tamper-proof [7].

This architecture enables real-time automation, cross-organisational data synchronisation, and trustless collaboration among stakeholders without dependence on a central authority. Moreover, since IPFS content addressing is hash-based, the system can verify whether data has been altered at any point in the supply chain. Overall, the integration supports a secure, scalable, and decentralised traceability model suitable for dynamic and compliance-sensitive logistics environments [16].

## RELATED WORKS

Several studies have investigated the integration of Blockchain-IoT to enhance traceability, accountability, and trust within logistics and supply chain operations [5],[7],[17]-[21]. Public blockchain platforms, such as Ethereum, remain popular due to their transparency and immutability. For instance, [7] and [19] propose combining Ethereum with IPFS to manage sensor data more efficiently. However, these approaches primarily focus on static data anchoring, offering limited flexibility for real-time event processing. Moreover, they often neglect enterprise privacy requirements, as public blockchains expose metadata and access histories to all network participants.

Another recurring limitation in public blockchain-based models is the latency of performance. Ethereum-based implementations often experience transaction bottlenecks due to network congestion and PoW consensus delays, making them unsuitable for time-sensitive logistics scenarios. Furthermore, these models generally lack fine-grained access control and support only simplistic smart contract logic, typically restricted to fixed data recording or binary rule enforcement. This reduces their adaptability in complex, event-driven workflows common in cold chain and multi-party logistics environments.

In contrast, permissioned blockchains, such as HLF, offer more suitable architectural foundations for enterprise-grade systems. For example, [20] utilises IoT sensors in conjunction with HLF to detect and log packaging breaches. While this demonstrates real-time event capture, it fails to incorporate decentralised storage or advanced smart contract capabilities. Similarly, other studies [13]-[14] explore RFID, BIM, and sensor-based IoT integration but rely heavily on centralised off-chain storage, raising concerns around data auditability and resilience.

A notable gap across much of the literature is the absence of holistic performance evaluation. Many works report only isolated figures, such as TPS or block size, without examining latency, fault tolerance, or throughput under real-world operational loads. Furthermore, smart contract design remains underutilised, often limited to basic rule enforcement without support for dynamic SLA triggers, multi-condition verification, or cross-chain interoperability.

As summarised in Table 1, this study advances the state of the art by integrating context-aware IoT sensing, a hybrid on/off-chain storage strategy using IPFS, and modular smart contracts that support fine-grained event validation. Unlike prior frameworks, the proposed solution combines high scalability, access control enforcement, and realistic benchmarking using Hyperledger Calliper, making it suitable for deployment in real-world logistics chains, particularly those that require compliance assurance, data resilience, and system-wide visibility.

## METHODS

### The Proposed Framework Overview

The BC-IoT-IPFS framework is built on a layered architecture that combines real-time sensing, secure BC validation, and decentralised off-chain storage to enable end-to-end logistics traceability. It brings together three core modules, an IoT deployment layer, a BC data management layer, and an IPFS-based storage layer, each playing a distinct role in ensuring trust, scalability, and data verifiability.

At the base, the IoT Deployment Module handles data sensing and edge-level processing. The module is structured into four logical layers. The Perception Layer captures raw logistics signals using embedded sensors, RFID tags, and actuators. These devices feed data to the Communication Layer, where wireless gateways and M2M protocols handle secure transmission. Data is then

**Table 1** Comparative summary of BC-IoT traceability

| Study | BC Type | IoT Integration | Storage Mechanism | Smart Contract Usage | Scalability & Privacy | Traceability Scope | Evaluation Method | Application |
|---|---|---|---|---|---|---|---|---|
| [7] | Public (Ethereum) | Multi-sensor + IPFS | Hybrid (on/off-chain) | Static logging only | Moderate; lacks ACL | End-to-end | Basic TPS tests | Logistics |
| [17] | BC + BIM | IoT with BIM | Centralised off-chain | Workflow automation | High, but not scalable | Component-level | Conceptual model | Offsite Manufacturing |
| [18] | Public BC | Embedded HMI sensors | Fully on-chain | Rule-based traceability | Low; weak endpoints | Farm-to-warehouse | Field test | Agriculture |
| [19] | Ethereum + IPFS | Sensor + metadata | Off-chain (IPFS) | Event recording | High; lacks privacy model | Ledger-level | Storage analysis | Generic use |
| [21] | Public BC | IoT for cold-chain | Fully on-chain | Monitoring triggers | Moderate; limited detail | Item-level | Conceptual model | Med-logistics |
| [5] | Solana | IoT sensing | On-chain | Transactional logging | Moderate; unclear ACL | Full-chain | Prototype | |
| This Study | Fabric (Permissioned) | Context-aware sensing | Hybrid: on-chain + IPFS | Modular smart contracts | High scalability + ACL | Full-chain + triggers | Realistic benchmarking | General |

passed to the Data Management Layer, which performs aggregation, local analytics, and event detection. At the top, the Application Layer exposes APIs and interfaces that allow external systems to interact with the captured data or initiate traceability actions. Once the data reaches the BC Data Management Module, it is submitted to an HLF network for secure validation. This layer is responsible for smart contract execution, ledger synchronisation, and identity management through MSPs and certificate authorities. Every logistics event, whether it is a custody transfer or a temperature breach, is immutably recorded and made accessible to authorised participants using private channels.

To prevent the blockchain from becoming overloaded with large payloads, IPFS was integrated as an off-chain storage layer. When a data file is uploaded to IPFS, the system generates a cryptographic hash (CID), which is then recorded on the BC. This approach ensures that sensitive files, such as sensor logs or compliance reports, remain verifiable and tamper-proof, without consuming excessive BC resources. The framework also supports cross-actor collaboration among carriers, manufacturers, regulators, and consignees. Smart contracts define transaction rules, detect anomalies, and trigger automated alerts to ensure seamless transactions. As shown in Figure 1, the entire system is designed to maintain traceability across the product lifecycle, from raw material sourcing to final delivery, while ensuring integrity, transparency, and operational efficiency [22].

**Implementation Workflow**

The BC-IoT-IPFS framework was implemented in three coordinated phases, each designed to ensure functional integrity, secure data flow, and robust performance under logistics-like workloads. The entire process is illustrated in Figure 2. In the first phase, a permissioned BC network using HLF was initialised. This setup included three organisations, each managing multiple peers, with certificate authorities (CAs) generating digital identities for trusted actors. Smart contracts, also known as chaincode, were deployed to enforce key logistics actions such as shipment registration, milestone confirmation, and anomaly detection. Simulated IoT events were streamed via MQTT and submitted to the BC through a RESTful API gateway built in Node.js. Once the blockchain layer was stabilised, the second phase focused on integrating off-chain storage using IPFS. When an IoT device detected a relevant event, the corresponding data payload, such as a temperature log or location report, was uploaded to IPFS. The system then generated a unique content identifier (CID), which is recorded on the BC alongside other metadata. This mechanism anchored the off-chain file in a tamper-evident way, ensuring that any future access or verification could be traced directly through the BC.

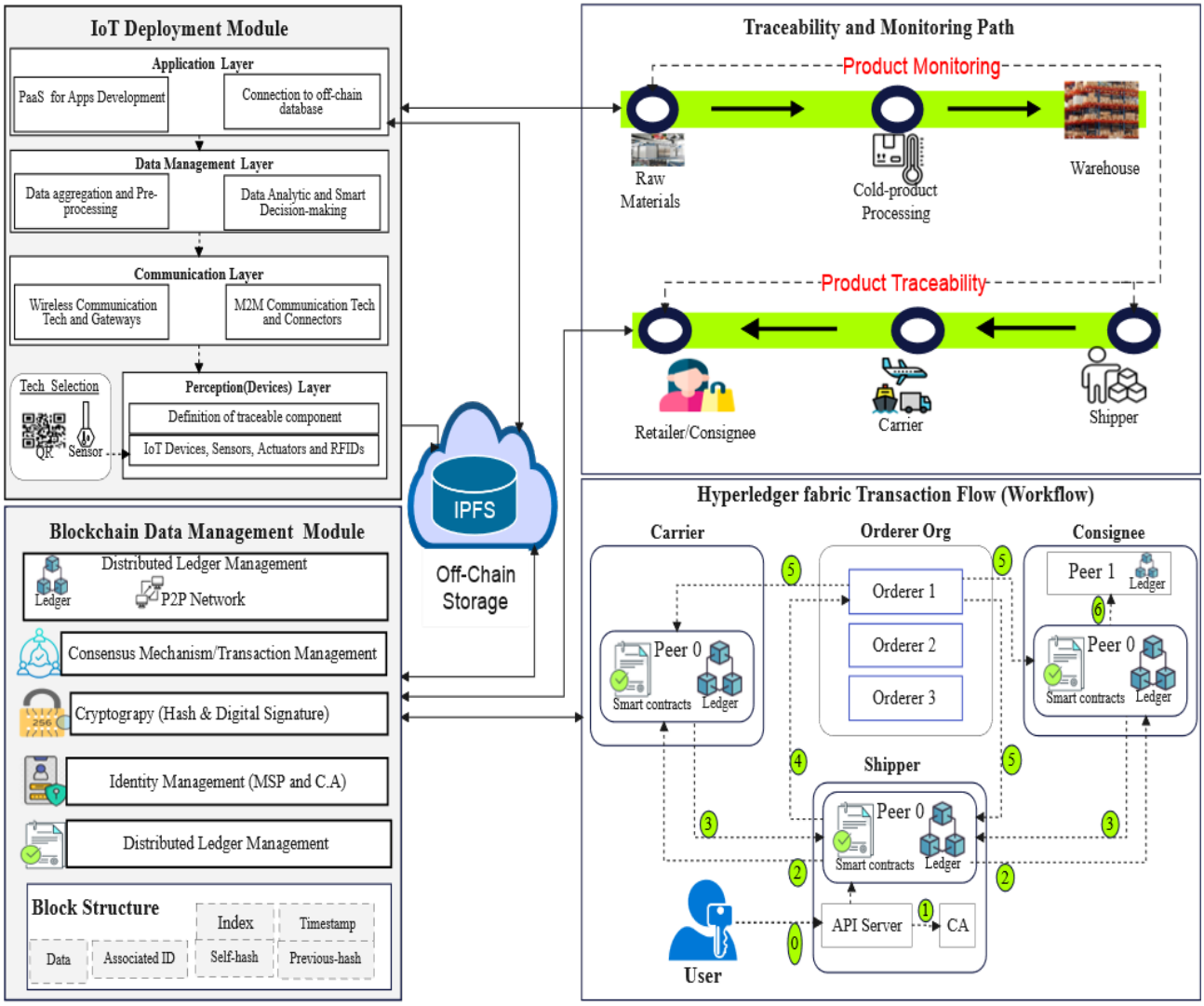


**Figure 1** Proposed BC-IoT-IPFS architecture with modular IoT sensing, BC validation, and IPFS-based off-chain storage

In the final phase, system performance was evaluated using Hyperledger Calliper. Mixed workloads, including read-heavy and write-heavy operations, were simulated under varying transaction volumes. Key performance indicators, including throughput, average latency, and transaction success and failure rates, were measured. These tests enabled fine-tuning of the configuration and validated the system's readiness for deployment in real-world logistics environments.

## EXPERIMENTAL EVALUATION AND DISCUSSION

### Evaluation Setup

To validate the performance of the proposed framework, we deployed a test environment configured with HLF v2.5.9 and go-IPFS. The system simulated a multi-organisational logistics network where IoT events, such as temperature breaches and dispatch milestones, were transmitted via MQTT and submitted to the BC through a Node.js REST API. Smart contracts were implemented in Go to support modular event handling.

Performance was evaluated using Hyperledger Calliper under write-intensive (Create Asset Operations, CAO) and read-intensive (Query Asset Operations, QAO) scenarios. The key setup parameters are summarised in Table 2. This configuration allowed for realistic emulation of a distributed logistics scenario, including event verification, off-chain storage integration, and performance stress testing.

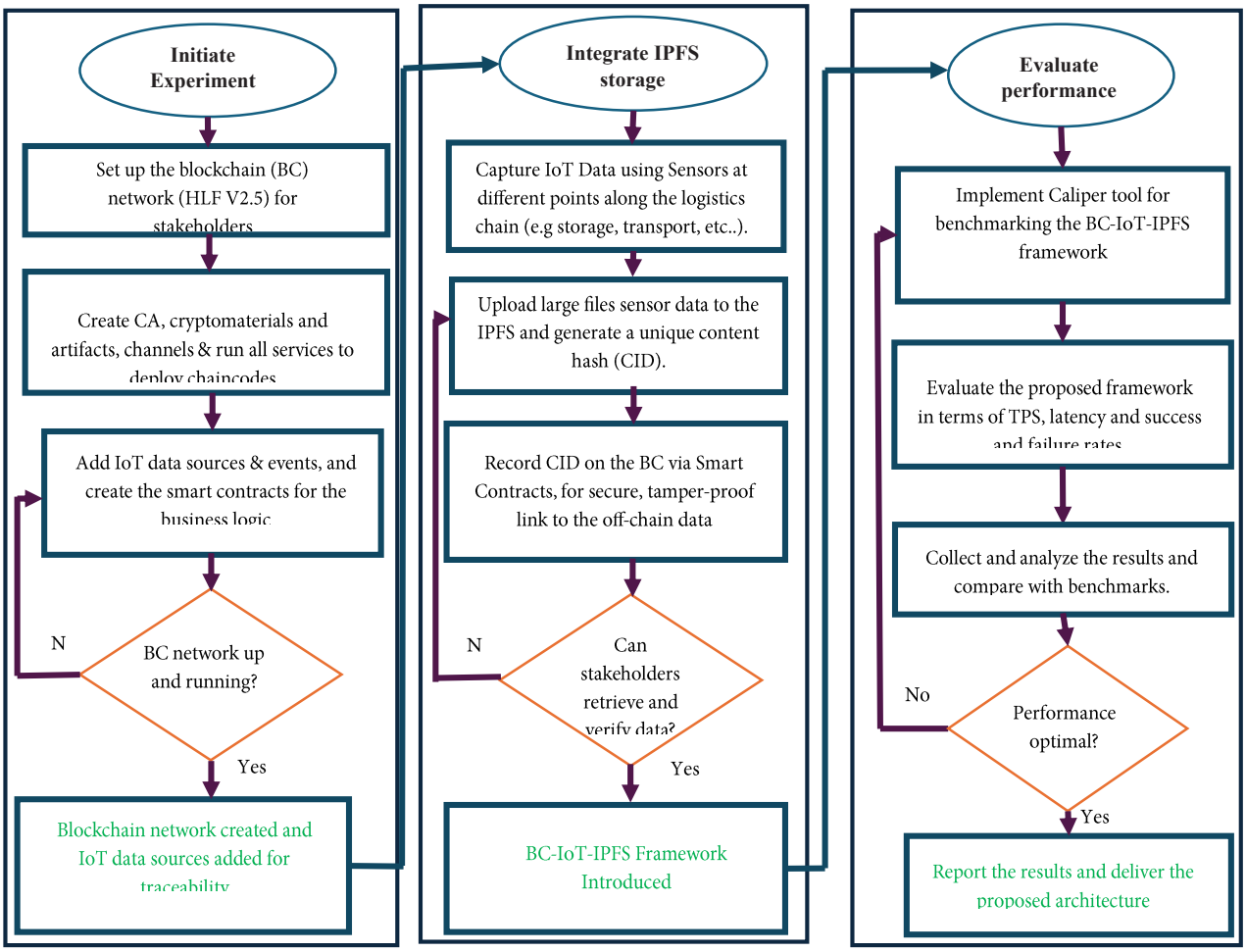


**Figure 2** Stepwise implementation workflow for the BC-IoT-IPFS framework

**Table 2** Experimental configurations

| Parameter | Value |
|---|---|
| OS | Ubuntu 24.04 (WSL) |
| BC Framework | HLFv2.5.9 |
| Consensus | RAFT |
| CPU | Multi-core (x86_64) |
| RAM | 16 GB |
| Storage | 50 GB SSD (Docker) |
| Smart Contract Language | Go (or Node.js) |
| Off-Chain Database | MongoDB |
| IPFS Version | go-IPFS (latest) |
| Benchmark Tool | Hyperledger Caliper |

## Performance Metrics

To evaluate the effectiveness and operational readiness of the proposed framework, a set of key performance metrics was defined to reflect responsiveness, scalability, and reliability. These include transaction throughput, latency, and success/failure rates under varying workloads. Table 3 summarises the formulas and descriptions for each metric used in the benchmarking process.

## Performance Results and Analysis

The proposed framework was evaluated based on three primary performance metrics: transaction success rate, latency, and throughput, under varying sending rates for both write-intensive (CAO) and read-intensive (QAO) scenarios. These test cases were designed to simulate real-world supply chain operations involving frequent event logging (CAO) and high-frequency querying (QAO).

As illustrated in Figure 3, throughput analysis confirms the framework's scalability. Under CAO (Figure 3a) conditions, throughput stabilised between 99 and 125 TPS, with performance plateauing around 100 TPS, which reflects the typical upper limit for blockchain write operations under permissioned settings. In contrast, QAO (Figure 3b) workloads demonstrated

**Table 3** Performance evaluation metrics

| Metric | Formula | Description |
|---|---|---|
| Throughput (TPS) | $\text{TPS} = \frac{\sum T_n}{t}$ | Measures how many transactions are successfully committed per second, indicating system scalability. |
| Latency (s) | $\text{Latency} = T_{\text{conf}} - T_{\text{sub}}$ | Captures the delay between submission and confirmation. Lower latency enables real-time traceability. |
| Success Rate (%) | $\text{Success Rate} = \frac{n_{\text{succ}}}{\sum T} \times 100$ | Indicates reliability by showing the percentage of transactions processed successfully. |
| Failure Rate (%) | $\text{Failure Rate} = \frac{n_{\text{fail}}}{\sum T} \times 100$ | Identifies system fragility by showing the proportion of failed transactions under load. |


**Figure 3** Sending rate versus Achieved TPS for (a) CAO (3000 transactions) and (b) QAO (5000 transactions) workloads

significantly higher efficiency, achieving up to 740 TPS at 800 tx/s, and maintaining a consistent throughput above 460 TPS across all tested sending rates. This indicates the framework's strong suitability for data retrieval-intensive operations such as compliance audits or SLA verifications.

In terms of transaction success rate presented in Figure 5, the system showed near-perfect reliability. For CAO (Figure 4a) a 100% success rate was maintained up to 130 tx/s, with minimal failures occurring only at the 140 tx/s threshold. Meanwhile, QAO workloads sustained full success rates up to 500 tx/s, with marginal degradation observed at higher loads, culminating in 436 failed transactions at the peak 800 tx/s rate. These results suggest that while the system can handle intensive read operations with minimal degradation, write-heavy conditions may require transaction queueing or throttling strategies under extreme loads.

Latency behaviour, presented in Figure 4, further differentiates the two workloads. Under CAO, latency increased proportionally with the sending rate, with the average delay rising from 0.18 seconds to 2.65 seconds, and peak latency reaching 8.9 seconds at a sending rate of 140 tx/s. This trend aligns with typical blockchain write bottlenecks, where block confirmation delays impact end-to-end responsiveness. Conversely, QAO scenarios maintained remarkably low latency, with average delays consistently below 30 milliseconds, regardless of input load. This responsiveness is essential for real-time, query-driven traceability, especially in cold chain or high-frequency logistics environments.

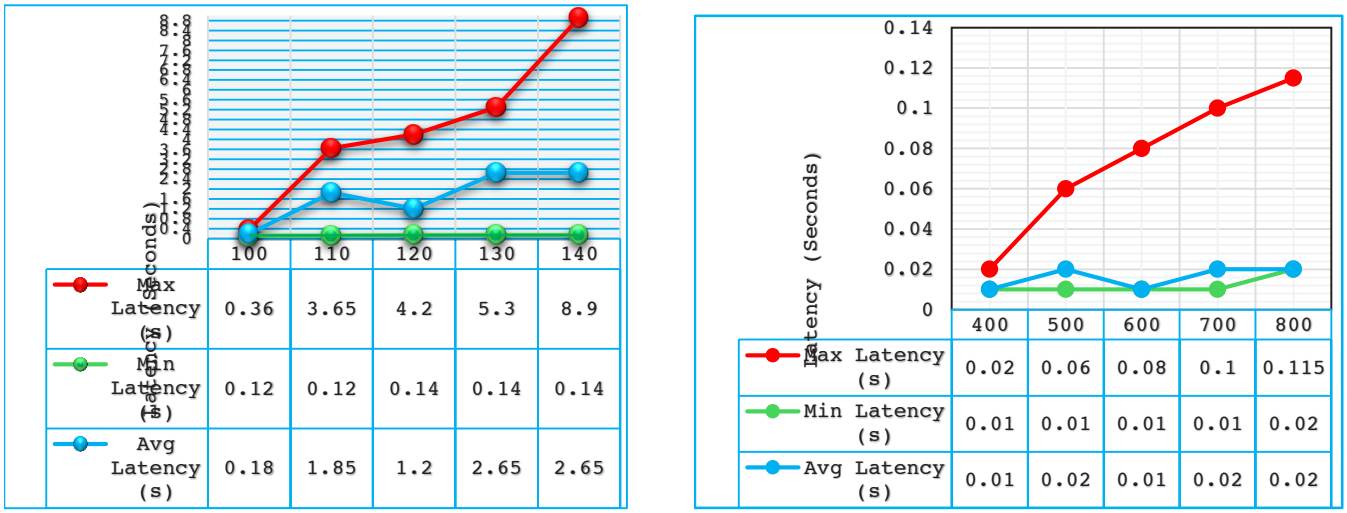


**Figure 4** Latency performance for (a) CAO and (b) QAO workloads, illustrating maximum, average, and minimum delays

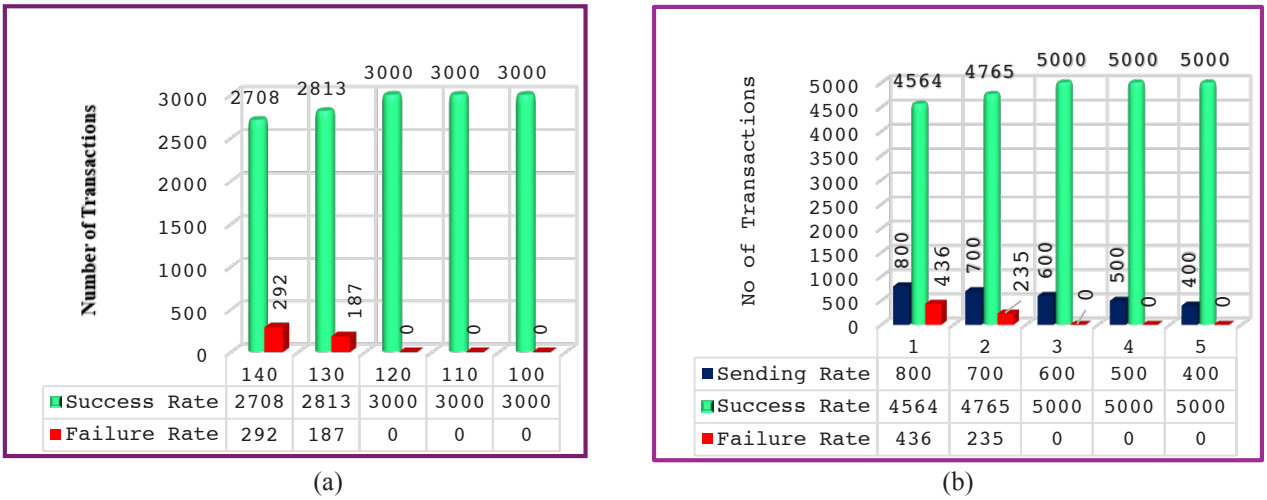


**Figure 5** Transaction success and failure rates under (a) CAO (3000 transactions) and (b) QAO (5000 transactions) workloads at varying sending rates

Overall, the experimental results validate the framework's ability to support both event-intensive data logging and high-performance querying with a high degree of reliability and responsiveness. The performance under QAO scenarios in particular highlights the architecture's scalability, low-latency capability, and operational viability in traceability-critical logistics systems.

## DISCUSSION AND COMPARATIVE ANALYSIS

The proposed BC-IoT-IPFS framework outperforms existing HLF-based traceability systems across throughput, latency, concurrency, and transaction reliability, as shown in Table 4. It achieved up to 120 TPS for asset creation (CAO) and 568 TPS for queries (QAO), surpassing earlier benchmarks, such as ≤100 TPS in [18] and [23], and up to 454 TPS in [17]. Latency remained low, averaging under 1.0 seconds for CAO and below 120 ms for QAO, improving upon delays reported in [17] (up to 1.5 s and 0.51 s, respectively) and matching the fast query response noted in [24], which, however, lacked asset creation timing. Scalability was demonstrated with support for up to 500 concurrent users, aligning with [17] and exceeding the limits reported in [18] and [23], which stated ≤300 users or none at all. The framework also maintained near-100% success rates under optimal loads, with a success/failure ratio of>120/0 (CAO) and >600/0 (QAO), demonstrating better transaction reliability than prior

**Table 4** Comparative performance of the proposed framework and existing traceability frameworks

| Study | Year | Platform | CA TPS | QA TPS | Max CU | CA Lat. (s) | QA Lat. (s) | CA S&F | QA S&F | USC? |
|---|---|---|---|---|---|---|---|---|---|---|
| [23] | 2021 | HLF v1.4 | ≤100 | <300 | — | <1.30 | — | >100/0 | — | Yes |
| [24] | 2021 | HLF v1.4 | ≤100 | ≤250 | — | — | <.0.12 | — | >400/0 | Yes |
| [18] | 2022 | HLF v2.2 | ≤100 | ≤407 | ≤300 | — | <1.20 | — | — | Yes |
| [17] | 2024 | HLF v2.5.9 | ≤110 | ≤454 | ≤500 | <1.5 | <0.51 | — | — | Yes |
| This Work | — | HLF v2.5.9 | ≤120 | ≤568 | ≤500 | <1.0 | <0.12 | >120/0 | >600/0 | Yes |

HLF = Hyperledger Fabric; CA = Create Asset; QA = Query Asset; TPS = Transactions per Second; Lat. = Latency; CU = Concurrent Users; S&F = Success and Failure Rate; USC = Upgradable Smart Contracts

systems that experienced degradation under stress or omitted reliability metrics altogether.

These gains result from three integrated features: modular chaincodes for lightweight execution, IPFS-backed off-chain storage for reducing ledger bloat, and HLF's permissioned architecture with RAFT consensus and private channels for secure, stable multi-party operations.

**Broader Implications, Stakeholder Impact, and Deployment Feasibility**

The proposed BC–IoT–IPFS framework has implications that extend beyond technical performance. By combining permissioned blockchain, IoT sensing, and decentralised off-chain storage, it strengthens traceability, accountability, and tamper-evidence across logistics partners [2],[7]. This supports more reliable audits, faster dispute resolution, and targeted recalls in sensitive sectors such as cold-chain products, food logistics, and regulated commodities, in line with observations from prior blockchain-enabled traceability systems [2],[23]-[24]. At the same time, immutable logging reconfigures data power relations: while it discourages opportunistic behaviour, it also raises concerns about long-term surveillance of smaller actors and the fairness of permanently recording every deviation or delay. These risks underline the need for explicit governance rules on data access, retention, and responsibility among consortium members, especially in tightly regulated or data-intensive environments [3].

Regulatory and economic factors significantly influence the feasibility of deployment. The framework can facilitate compliance by providing verifiable records of custody, environmental conditions, and contract fulfilment. However, regulators must be able to map on-chain events and off-chain evidence to existing legal and documentation standards [2]-[3]. Economically, consortium-based deployments and the use of IPFS to offload large payloads can reduce ledger growth and infrastructure costs compared to fully on-chain designs, complementing earlier work that highlights the scalability benefits of hybrid blockchain–IPFS models in logistics [7]. However, capital and operational expenditures for running peers, IPFS nodes, and IoT gateways may still be significant, particularly for SMEs. A detailed cost–benefit analysis, including savings from reduced manual reconciliation and improved visibility, remains an important direction for future work [2].

The stakeholder impact of the framework is multifaceted. Manufacturers and brand owners gain stronger guarantees about product handling and can substantiate claims related to quality or compliance; logistics providers can differentiate services through auditable service-level adherence; regulators and auditors benefit from trustworthy, time-stamped histories; and end-users indirectly benefit from more transparent supply chains [2],[23]-[24]. Successful adoption, however, depends on stakeholder readiness, including digital literacy, process maturity, and willingness to share data under a shared governance and incentive model. These factors collectively determine whether the framework is not only technically sound but also socially and operationally feasible in real logistics ecosystems.

**Limitations and Future Work**

The present study is confined to controlled, Calliper-based benchmarking of the proposed BC–IoT–IPFS framework and does not yet incorporate user or stakeholder validation through real-world pilots. As a result, the findings primarily demonstrate technical feasibility in terms of performance and functionality, rather than full organisational or socio-technical integration within live logistics operations. In addition, the current prototype focuses on core traceability, data management, and performance evaluation,

without embedding advanced AI modules for anomaly prediction or automated service-level assessment, and without implementing cross-chain interactions with external blockchain networks.

Future work should therefore prioritise pilot deployments with selected logistics partners, complemented by stakeholder interviews and co-design workshops to examine usability, data-governance concerns, and perceived value in practice. Such empirical investigations would provide richer insights into adoption barriers and enablers, and would allow a more comprehensive assessment of the framework's practical feasibility and impact in operational logistics environments. On the technical side, further research could extend the framework with AI-driven anomaly prediction based on real-time IoT data streams, intelligent SLA monitoring to assess and enforce service-level commitments across logistics partners, and cross-chain interoperability mechanisms to link the core traceability ledger with sectoral or regulatory blockchains.

## CONCLUSION

This paper presented a decentralised framework that integrates BC, IoT, and IPFS to address key traceability challenges in modern logistics chains. By combining permissioned BC validation, real-time IoT sensing, and content-addressed off-chain storage, the proposed architecture ensures secure, scalable, and tamper-evident data flow across multiple actors and stages of the supply process. Our implementation demonstrated that this hybrid model significantly reduces BC storage overhead while maintaining data integrity and performance. Experimental results demonstrated low latency, high throughput, and robust resistance to common attack vectors, making it a practical solution for logistics scenarios that require transparency, speed, and verifiability. Looking ahead, the proposed framework lays the groundwork for more intelligent and accountable supply chain systems, supporting service-level monitoring and interoperable traceability across regulatory, agri-food, and pharmaceutical domains.

## ACKNOWLEDGMENT

The author gratefully acknowledges the support of Universiti Teknologi PETRONAS (UTP) for providing the research environment, facilities, and academic mentorship essential to the successful completion of this study. Special thanks are also extended to the Petroleum Technology Development Fund (PTDF), Nigeria, for the award of a postgraduate scholarship, which significantly contributed to the funding and continuity of this research work.

## REFERENCES

[1] C. Wang, X. Sang, and L. Gao, "A Cross-chain Gateway for Efficient Supply Chain Data Management," in *Communications in Computer and Information Science*, W. Gao et al., Eds., School of Software Engineering, Xi'an Jiaotong University, Xi'an, 710049, China: Springer Science and Business Media Deutschland GmbH, 2021, pp. 318–333. doi: 10.1007/978-981-16-1160-5_25.

[2] Y. Saidu, S.M. Shuhidan, I.A. Aziz, M.M. Alam, D.A. Aliyu, and M.M. Yakubu, "Exploring Blockchain–IoT Convergence for Logistics Traceability: A Systematic Review and Future Outlook," *IEEE Access*, pp. 112390-112416, 2025, doi: 10.1109/ACCESS.2025.3583927.

[3] U. Majeed, L.U. Khan, I. Yaqoob, S.M.A. Kazmi, K. Salah, and C.S. Hong, "Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges," *J. Netw. Comput. Appl.*, vol. 181, p. 103007, May 2021, doi: 10.1016/j.jnca.2021.103007.

[4] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-Based Soybean Traceability in Agricultural Supply Chain," *IEEE Access*, vol. 7, pp. 73295–73305, 2019, doi: 10.1109/ACCESS.2019.2918000.

[5] M. Ashraf and C. Heavey, "A Prototype of Supply Chain Traceability using Solana as blockchain and IoT," *Procedia Comput. Sci.*, vol. 217, pp. 948–959, 2022, doi: 10.1016/j.procs.2022.12.292.

[6] T.V. Doan, Y. Psaras, J. Ott, and V. Bajpai, "Toward Decentralized Cloud Storage With IPFS: Opportunities, Challenges, and Future Considerations," *IEEE Internet Comput.*, vol. 26, no. 6, pp. 7–15, Nov. 2022, doi: 10.1109/MIC.2022.3209804.

[7] N.A. Ugochukwu, S.B. Goyal, A.S. Rajawat, C. Verma, and Z. Illes, "Enhancing Logistics With the Internet of Things: A Secured and Efficient Distribution and Storage Model Utilising Blockchain Innovations and Interplanetary File System," *IEEE Access*, vol. 12, no. September 2023, pp. 4139–4152, 2024, doi: 10.1109/ACCESS.2023.3339754.

[8] Y. Saidu, S.M. Shuhidan, I.A. Aziz, D.A. Adamu, S. Yau, and S. Adamu, "A Bibliometric Analysis on Blockchain Consensus Algorithms: Unveiling Trends, Contributors, and Intellectual Structures," in *Proceedings of the International Conference on Smart Cities - Volume 2 ICSC 2024, September 10-11, Kota Kinabalu, Malaysia*, M. Hisham, H. Mohd Hilmi, A. Said Jadid, and S. Nasir, Eds., Singapore: Springer Singapore, 2025, pp. 579–593. doi: 10.1007/978-981-96-5848-0_47.

[9] E. Androulaki, A. Barger, V. Bortnikov,..., S.W. Cocco, and J. Yellick, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proc. 13th EuroSys Conf. EuroSys 2018*, vol. 2018-Janua, 2018, doi: 10.1145/3190508.3190538.

[10] J. Polge, J. Robert, and Y. Le Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Express*, vol. 7, no. 2, pp. 229–233, Jun. 2021, doi: 10.1016/j.icte.2020.09.002.

[11] A.A. Monrat, O. Schelen, and K. Andersson, "Performance Evaluation of Permissioned Blockchain Platforms," in *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering, CSDE 2020*, IEEE, Dec. 2020, pp. 1–8. doi: 10.1109/CSDE50874.2020.9411380.

[12] S. Nanayakkara, M.N.N. Rodrigo, S. Perera, G. T. Weerasuriya, and A. A. Hijazi, "A methodology for selection of a Blockchain platform to develop an enterprise system," *J. Ind. Inf. Integr.*, vol. 23, no. 100215, pp. 1–16, Sep. 2021, doi: 10.1016/j.jii.2021.100215.

[13] C.-L. Chen, X. Shang, W.-J. Tsaur, W. Weng, Y.-Y. Deng, C.-M. Wu, and J. Cui, "An anti-counterfeit and traceable management system for brand clothing with hyperledger fabric framework," *Symmetry (Basel)*, vol. 13, no. 11, pp. 1–32, 2021, doi: 10.3390/sym13112048.

[14] S. Yau, A. Aliyu, Y. Saidu, A. Ibrahim, and F. M. Aliyu, "Prospect of Smart Agriculture Using IoT and Data Analytics: A Perspective of Kebbi State, Northwestern Nigeria," *Int. J. Adv. Netw. Appl.*, vol. 15, no. 06, pp. 6194–6203, 2024, doi: 10.35444/ijana.2024.15606.

[15] B. Subashini and D. Hemavathi, "Scalable Blockchain Technology for Tracking the Provenance of the Agri-Food," *Comput. Mater. Contin.*, vol. 75, no. 2, pp. 3339–3358, 2023, doi: 10.32604/cmc.2023.035074.

[16] Y. Saidu, S.M. Shuhidan, D.A. Aliyu, I.A. Aziz, and S. Adamu, "Convergence of Blockchain, IoT, and AI for Enhanced Traceability Systems: A Comprehensive Review," *IEEE Access*, vol. 13, pp. 16838–16865, 2025, doi: 10.1109/ACCESS.2025.3528035.

[17] R. Brandín and S. Abrishami, "IoT-BIM and blockchain integration for enhanced data traceability in offsite manufacturing," *Autom. Constr.*, vol. 159, no. 105266, pp. 1–24, Mar. 2024, doi: 10.1016/j.autcon.2024.105266.

[18] F.J. Ferrández-Pastor, J. Mora-Pascual, and D. Díaz-Lajara, "Agricultural traceability model based on IoT and Blockchain: Application in industrial hemp production," *J. Ind. Inf. Integr.*, vol. 29, no. July 2022, pp. 1–15, 2022, doi: 10.1016/j.jii.2022.100381.

[19] R. Kumar, N. Marchang, and R. Tripathi, "SMDSB: Efficient Off-Chain Storage Model for Data Sharing in Blockchain Environment," in *Advances in Intelligent Systems and Computing*, D. Swain, P.K. Pattnaik, and T. Athawale, Eds., Springer Science and Business Media Deutschland GmbH, 2021, pp. 225–240. doi: 10.1007/978-981-33-4859-2_24.

[20] M. Balfaqih, Z. Balfagih, M. D. Lytras, K. M. Alfawaz, A. A. Alshdadi, and E. Alsolami, "A Blockchain-Enabled IoT Logistics System for Efficient Tracking and Management of High-Price Shipments: A Resilient, Scalable and Sustainable Approach to Smart Cities," *Sustain.*, vol. 15, no. 13971, pp. 1–18, Sep. 2023, doi: 10.3390/su151813971.

[21] W. Zeng, Y. Wang, K. Liang, J. Li, and X. Niu, "Advancing Emergency Supplies Management: A Blockchain-Based Traceability System for Cold-Chain Medicine Logistics," *Adv. Theory Simulations*, vol. 7, no. 4, pp. 1–18, 2024, doi: 10.1002/adts.202300704.

[22] Y. Saidu, M. S. Shuhaida, A.A. Dahiru, S. Yau, M. Y. Muhammad, and A.A. Babando, "Charting the Course : A Bibliometric Exploration of Blockchain Traceability Systems," in *International Conference on Technological Solutions for Smart Economy*, 2024, pp. 1–8. [Online]. Available: https://library.ncs.org.ng/download/charting-the-course-a-bibliometric-exploration-of-blockchain-traceability-systems/.

[23] Y. Zhang, Y. Liu, Z. Jiong, X. Zhang, B. Li, and E. Chen, "Development and assessment of blockchain-IoT-based traceability system for frozen aquatic product," *J. Food Process Eng.*, vol. 44, no. 5, pp. 1–14, May 2021, doi: 10.1111/jfpe.13669.

[24] X. Yang, M. Li, H. Yu, M. Wang, D. Xu, and C. Sun, "A Trusted Blockchain-Based Traceability System for Fruit and Vegetable Agricultural Products," *IEEE Access*, vol. 9, pp. 36282–36293, 2021, doi: 10.1109/ACCESS.2021.3062845.