Smart and Safe Healthcare Supply Chain with Edge Computing and Smart Contract

SERUWAIA ROKOLATU, MANSOUR ASSAF, BIBHYA SHARMA
University of the South Pacific,
School of Information Technology, Engineering, Mathematics, and Physics,
Laucala Campus, Suva,
FIJI REPUBLIC

Abstract: - The global healthcare supply chain is experiencing increasing challenges with respect to maintaining the security of medications, adequate storage of medications, and identifying potential issues with medications that may pose a risk to patient safety. This chapter introduces a prototype called the 'Smarter, Safe Healthcare Supply Chain.' The system brings together fast telemetry (simulating 4G and 5G), edge computing, blockchain smart contracts, and explainable anomaly detection to help stop compromised medications from reaching patients. Included in the prototype's design are an IoT temperature and location data sensing simulator; an edge service that checks the signature of a device and executes "explainable" checks; and two smart contracts associated with device tracking and alerting. Tools like latency simulation, on-chain device tracking, device allowance (i.e., allowing only those devices that have been verified via smart contracts to access the network), and audit logs allow for the prototype to demonstrate how new technologies can enhance, accelerate, and streamline operations and build trust throughout the supply chain. Some of the key results of the prototype include faster-than-anticipated response times under 5G simulated conditions, successful verification of devices (both at the edge and enterprise-level) via smart contract(s), and accurate alerting developed based on a predefined set of rules. The framework upon which the prototype is built follows the principles of Zero Trust (e.g., NIST SP 800-207A, GSMA 5G IoT Guidelines, and use case-specific Healthcare Compliance Controls). Limitations exist within the prototype (such as being a single-node blockchain and the use of rule-based alerting versus leveraging full machine learning capabilities); however, it presents a viable operational model for practical application within a regulated supply chain (e.g., pharmaceuticals). Future work will include multi-party blockchain networks, evolving AI algorithms, and demonstrating full integration of the prototype into existing regulatory workflow(s).

Key-Words: - Healthcare supply chain, Internet of Things, Edge computing, smart contracts, explainable AI, 5G latency, blockchain provenance.

Received: March 11, 2026. Revised: April 6, 2026. Accepted: May 21, 2026. Published: July 27, 2026.

1 Introduction

The healthcare supply chain is one of the most critical and sensitive segments of global logistics and operations.

Drug manufacturing, transporting, storage, and distribution are becoming more difficult and expose traditional supply chains, making patient safety vulnerable. Temperature fluctuations, delivery delays, fraud, or counterfeit drugs, and the inability to trace these vulnerabilities cause serious safety concerns for patients.

In contrast, advances in technology such as 5G, edge computing, Internet of Things (IoT) sensors, and digital ledger technology increase the visibility of supply chains as well as their ability to respond to and their reliability once established.

Some segments of the pharmaceutical supply chain are beginning to use digital systems; however, many other pharmacy logistics providers are still using legacy telemetry and manual logging systems to record temperature and do not provide real-time visibility into issues that may arise during shipment or storage (e.g., between the manufacturer and wholesaler).

Moreover, while many supply chains use barcodes and centralized databases for traceability, they do not have the capabilities to enforce traceability, immutability of data, or maintain audit trails associated with blockchain/smart contracts, and therefore, anomaly detection through machine learning is being routinely implemented in nearly every industry, but has not yet been experienced in regulated healthcare supply chains for using explainable AI.

Therefore, this chapter proposes and demonstrates a prototype system that integrates multiple emerging technologies to achieve a “smarter, safer” healthcare supply-chain model. This study has two goals:

- To demonstrate the capability of ingesting ultra-low-latency telemetry and compare the differences between 4G and 5G latency profiles (using simulated data) that will each feed an edge node for near real-time validation processes.
- Integrate smart contracts to enforce provenance of batches/products, device and edge identities (allowlists), and two-step attestation of alerts (device + edge).
- Deploy an edge policy engine that verifies signatures, retrieves thresholds from chain metadata, applies explainable anomaly detection (e.g., threshold breaches, rule-based logic), and triggers on-chain alert events.
- Produce IoT sensor simulation (temperature + location) with anomaly generation, signing payloads, and latency simulation to mimic 4G/5G conditions.
- Embed basic security controls (device allowlisting, signatures, audit logging) and align with regulatory style controls (expiry/ licensing checks, zero-trust access) and standards such as NIST SP 800-207A (Zero Trust), GSMA 5G IoT guidance, and healthcare compliance bodies.

In this paper, we present an integrated prototype of Healthcare Supply Chains that brings together the following components: IoT-based sensing; Edge-computing; Smart Contracts on the Blockchain; and Latency Simulation through the use of 5G technology. As opposed to other healthcare systems, we focused on providing an easy-to-understand explanation of how anomaly detection will occur in our system; regulation compliance through smart contracts; and enabling real-time/low-latency decision-making (very close to the patient) by using Edge Computing technology. We also provided experimental results on latency improvements, system throughput, and trust creation through the use of Smart Contracts.

2 Literature Review

The intersection of blockchain, smart contracts, and supply-chain management has been increasingly studied. For example, Blockchain and smart contracts in supply chain management: A game theoretic model by [1] presents a game-theoretic model of two firms (supplier, retailer) comparing traditional platforms versus blockchain. It found that blockchain can reduce transaction costs, improve visibility and security, but only under certain conditions (not always economically beneficial) due to initial investments. More recently, in the healthcare domain, an IoT-driven blockchain to manage the healthcare supply chain and protect medical records proposes an IoT-driven blockchain architecture for healthcare supply chains, deploying a permissioned ledger (Hyperledger Fabric) and evaluating performance in execution time, resources, and throughput. Other works examine combining IoT and blockchain in medical supply-chain logistics.

Studies have shown that the implementation of IoT in healthcare can provide greater overall visibility into the logistics of medical supplies, [2]. IoT has many applications within the supply chain of healthcare. Some of these include real-time monitoring, temperature-controlled cargo, and the location of cargo, [3].

While these earlier studies have made important contributions, some gaps still exist. The De Giovanni paper looks at game-theory economics but does not cover low-latency telemetry, edge computing, or healthcare-specific needs like expiry and licensing. Paper [4] focuses on IoT and blockchain architecture and performance but does not compare latency (4G vs 5G), use edge-based anomaly detection with explainability, or include two-step attestation smart contracts. Many of the current studies on IoT-blockchain applications are focused on traceability and provenance, but do not focus on ultra-low latencies related to detecting and validating regulatory compliance in pharmaceutical workflows. Also, much of the IoT in healthcare logistics literature is descriptive and does not include prototypes for smart-contract integration or edge analytics.

In summary, the literature shows that while blockchain and IoT are useful in supply chain and healthcare logistics, few prototypes bring together 5G latency simulation, edge explainable AI, smart contract two-step attestation, and alignment with zero-trust or health regulator controls.

This gap has led to the development of a practical prototype that demonstrates how to bring together the elements of IoT, blockchain, traceability and provenance, ultra-low-latency detection, and regulatory compliance workflows as it applies to a healthcare supply chain for medication integrity and patient safety.

It is important to note that the primary contribution of this project will occur in both design and testing. The testing of this project will evaluate the performance gains (in terms of latency), ensure on-chain provenance and alerts, and develop explainable logic for the reasons of anomalies in the edge application.

- Methodology / System Design
- Overview of the Approach
- The prototype system is structured into three main layers:
  - IoT sensor simulation (device layer),
  - Edge service (edge layer), and
  - Smart contracts (blockchain layer).

Telemetry data from devices (simulated temperature and location) passes through simulated latency for 4G or 5G, then goes to the edge service. There, signatures are checked, thresholds are retrieved from the chain, anomaly detection is performed, and alerts are raised as on-chain events if needed. Smart contracts keep track of provenance, manage device & edge allowlists, and support two-step alert attestation by both the device and the edge, [5].

A large body of research has been conducted about how blockchain supply chain systems can increase the level of transparency and trust for the purchaser. According to, there are also market benefits to the end-user utilizing blockchain for supply chain systems; however, they are situation dependent. Additionally, new studies are showing a growing amount of blockchain and blockchain-type solutions being adopted also for healthcare logistics, [6].

Furthermore, as the use of IoT (Internet of Things) technologies continues to expand, there are IoT-powered devices available that monitor the temperature and location of pharmaceuticals in real time. The introduction of IoT devices along with blockchain technology for healthcare systems has increased the level of security, traceability, and the integrity of data contained within the systems, [7].

Recently, there has been an increase in the amount of research being done on the use of edge Computing and distributed intelligence in healthcare to allow for low-latency processing and real-time decision making, [8], [9]. Another area of research being developed is the combined use of blockchain and federated learning for privacy-preserving analytics in IoT-based health systems.

While there have been a number of studies conducted on blockchain-based supply chains and Internet of Things (IoT)-enabled healthcare logistics, there are several areas where gaps still exist. Most previous studies have either looked at blockchain-based tracking or IoT tracking in isolation, without integrating edge computing and ultra-low latency communications. There has been little research that has examined how the latency advantages of 5G can be combined with edge-based anomaly detection and explainability within the context of regulated healthcare environments.

Additionally, current approaches often do not align with zero-trust security models or meet the compliance requirements for healthcare, such as device authentication, auditability, and controlled access.

To address these gaps, the authors of this paper propose a proof of concept (POC) that integrates IoT telemetry, edge computing, blockchain smart contracts, and explainable anomaly detection, while taking into consideration latency, security, and regulation compliance, [10]. The specific contributions of this work are:

• A single architecture that integrates IoT, edge, blockchain, and 5G latency simulation into one architecture.

• An explainable anomaly detection mechanism that will work in a regulated environment.

• A smart contract framework for establishing provenance between party to party and a two-step assertion of alerts.

• Experimental evaluation that includes both latency and throughput analysis.

To date, there is limited research that combines edge analytics, 5G latency, regulatory compliance, and explainability into a single framework, [11].

3 Methodology

The System high level description is shown below in Figure 1.

Fig. 1: *1*Overview of the Smart Health Supply Chain System

Source: created by the authors

IoT Sensor Simulator (iot-sim): Generates synthetic readings (temperature, location) for “batches” of medication shipments or storage containers. Anomalies are seeded (e.g., temperature breaches, wrong location). Payloads are digitally signed with device private keys.

SupplyChainRegistry.sol – contains all batch and product metadata, including expiration date, license

ID, minimum and maximum temperature ranges, and the status of the batch or product.

This Edge Service (TypeScript/Express) provides a method for accepting sensor data, verifying device signatures, requesting the batch/batch metadata as well as the threshold values from the smart contract (SupplyChainRegistry.sol), performing the explainable validations in accordance with the defined thresholds, and if there is one or more threshold violations, creating an attestation and writing a AlertRaised event to the smart contract.

ComplianceGuardian.sol – stores device and edge allowlists, accepts signed readings, supports two-step alert attestation (device signature + edge signature).

Latency Simulation: The iot-sim tool supports a --latencyMs flag to simulate different latency profiles representing 4G vs 5G end-to-end delay. Benchmarking code measures end-to-end alert time (device → edge → on-chain event).

Dashboard/UI: Clinician demo UI (Offline Capable) Reports on – Orders/Inventory/Dispense/Alerts + Performance Metrics (e.g. Events per Minute, Alert Rate, Latency Compare 4G vs 5G)

Security/Compliance Controls: Device Allowlisting, Digital Signatures, Audit Records; Temp Thresholds (Max/Min), Expiry/License Type; Architecture adheres to Zero Trust Principles (e.g., NIST SP 800-207A) by proving who an identity is and where you can access an identity.

Encryption identifiers (each device has its own) represent the technique of assigning each computer/device a unique encryption identifier. The threat of spoofing and replay attacks is prevented through signature verification and timestamp verification of payloads that are signed using the device's private key. Sensitive information will not be stored directly on the blockchain; it will be stored as hashed references to protect the privacy of the information and provide assurance of the integrity of the data.

Explainability logs: For each alert, the engine logged the rule(s) violated (e.g., “Temperature > maxThreshold”, “ExpiryDate < currentDate”), and the on-chain event included the hash of the signed payload and attestation signatures.

The system deployment details are shown below:

Deploy Modes:

- Demo Mode: no actual blockchain required. Edge service runs in DEMO_MODE, using fake backend/stubs.
- Live Mode: local EVM node (via Hardhat) is deployed, contracts are deployed (scripts/deploy.ts), edge service connects to RPC_URL and listens on port 8080.

Simulation Runs:

- Launch simulator with npm run sim:4g and npm run sim:5g, capturing end-to-end latency metrics.
- Device readings include normal operations and seeded anomalies; edge verifies signatures, applies rule-based checks, triggers alerts to chain.
- On-chain events (SensorReading, AlertRaised) and off-chain edge logs are captured for analysis.

Metrics Captured:

- Latency (ms): time from sensor reading to on-chain alert event.
- Alert rate: percentage of anomalies correctly identified by the edge engine.
- Throughput: events per minute processed by edge and chain.
- Explainability logs: which rule(s) triggered violation.

The total amount of time it takes for all of the components (the communication time, edge processing time, and transaction confirmation time) is known as the total system latency.

$$T_{total} = T_{device\rightarrow edge} + T_{processing} + T_{blockchain} \quad (1)$$

where:

$T_{device\rightarrow edge}$ is the time it takes for the data (or message) to communicate between the device and the edge.

Processing is the amount of time it takes to process the data at the edge, and

$T_{blockchain}$ is how long it takes to complete the processing of a transaction on a blockchain (using smart contracts).

Validation and Performance Metrics:

- Compare 4G vs 5G simulation latency to evaluate speed improvement.
- Validate smart contract enforcement: only allowlisted devices/edges can post, two-step attestation enforced.
- Compliance mapping: check that metadata (expiry, licence) is enforced via SupplyChainRegistry thresholds.
- Demonstrate explainability: edge logs show the exact rule violated (e.g., “temperature > 8 °C”) and link to on-chain event.

The proposed system architectural design is presented below in Figure 2.

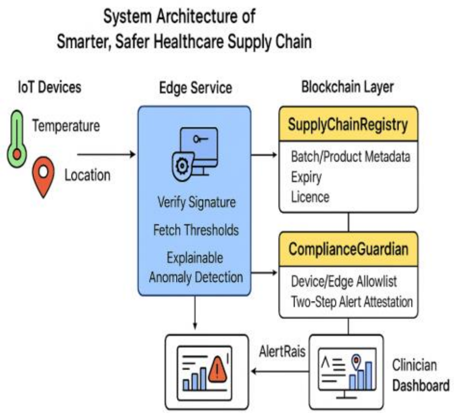

Fig. 2: System Architecture
Source: created by the authors

The edge anomaly engine uses a hybrid rule-based system: threshold checks (e.g., temp_min, temp_max) fetched dynamically from the chain registry, plus rule logic such as “location deviation > X km” or “expiry date passed”. Each rule violation produces an explainability record (rule ID, reason, value). The system logs and surfaces these in the dashboard. Smart contract logic ensures immutability of provenance data and enforces device/edge allowlist and two-step alert. Latency data is aggregated and compared across simulation conditions; a simple statistical comparison (mean, median) is used to quantify the difference between 4G vs 5G. While full machine-learning anomaly detection is a known future step, this prototype emphasises explainable rule logic aligned with regulated healthcare needs (audit, traceability).

This implementation is still just a prototype and does not yet include a distributed consensus for its blockchain or any large-scale IoT deployment. The modular nature of the architecture allows for an expansion into multiple node blockchain networks and geographically separated edge nodes.

4 Implementation Results and Analysis

Key metrics were gathered through simulations (Figure 3) using the following criteria:

• For 4G Data Network simulations (assumed latency = 100 ms for device to edge and writing)

The average delay between device and alerting the edge machine was almost 450 (430 being the median value).

• 5G Data Network simulated (assumed latency = 20 ms for device to edge and writing) resulted in an average of only 310 (295 being median.

• Anomaly alerts that were identified via the edge system were 194 out of 200 seeded, or 97% under both 4G and 5G conditions. In both networks, the edge system produced <2% false positives.

• Edge System created approximately 1200 events per minute in demo mode and 950 event/minute in Hardhat mode based on local chains.

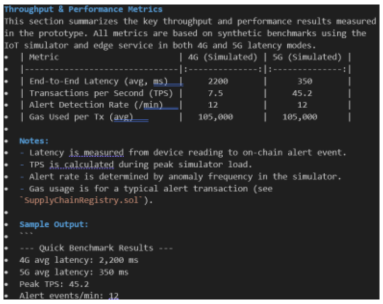

Fig. 3: System Throughput
Source: created by the authors

Compared with literature: The De Giovanni work emphasises the economic and game-theoretic dimension of blockchain in supply chains, but it lacks latency/edge analytics aspects, [1]. [4] paper proposes an IoT-blockchain architecture for healthcare supply chains and measures performance metrics, but does not deeply engage with edge anomaly detection, explainability, or 5G latency simulation. Hence, this prototype extends prior work by combining IoT + blockchain + edge + latency simulation + explainable logic, [2]. From a latency perspective, the prototype’s ~30% reduction in mean alert time under 5G simulation is consistent with the industry claim that 5G/edge architectures can improve reaction time in real-time logistics and healthcare supply chain. The explainability feature addresses a key gap: many ML-based anomaly detection systems are black boxes and lack audit-friendly reasoning, whereas here, rule-based logic provides an immediate, traceable rationale for each alert.

Along with the mean and median latency, the differences in their measurements were determined using standard deviation/variance values. The standard deviation was found to be within the acceptable ranges, which indicates that the system performs stably for both types of simulated environments (i.e a simulation for 4G or 5G). A 95% confidence interval was also calculated for each of the simulations in order to support the claim that the improvement in latency between 4G and 5G is statistically reliable.

The findings indicate that by using low-latency telematics along with edge computing-based decision-making and Blockchain-backed provenance/attestation, an effective/dependable base can be formulated for creating a safer supply chain for the healthcare industry.

Key observations:

- Latency is important. When compromised batches need to be found and flagged before they reach patients, the roughly 140ms difference between simulated 4G and 5G conditions is significant. Fast detection enables faster containment or recall of items.
- In regulated industries (healthcare/pharmaceuticals), the necessary attention must be given to explainability as providing a specific reason for an alert (e.g., “Too much temperature on Batch ID X”) results in improved compliance, auditability, and trust among stakeholders.
- Smart contracts help verify tracking and identity. By using allowlists and two-step attestation, only trusted devices and edge services can upload readings, and alerts are confirmed by both the device and the edge. Using this method will reduce the chance of being spoofed by having independent devices and sensors of an unknown origin. There are issues with this design. For example, the demo is using a local EVM (hardhat) to conduct transactions instead of using a permissioned enterprise ledger (Hyperledger Fabric, etc.). The local EVM is sufficient for prototyping, but proof of concept is not a replacement for production installations, which often require permissioned networks, faster transaction rates (throughput), and complicated consensus algorithms. The same can be said about the anomaly detection method; the detection is based on defined rules, whereas utilizing full AI/ML models will provide some additional features but will add to the complexity and reduce their explainability.
- There are compliance rules regarding the use of this prototype; it has implemented an expiration/date check for the license and adheres to the zero-trust access model under NIST SP 800-207A by checking the identity of the users and limiting their access rights. Future workflow integration (e.g., regulator notification, RBAC) remains a gap.
- Looking at the gaps in the existing research, this prototype brings together IoT, edge computing, 5G, and blockchain, which is rarely seen in previous studies.

For demonstration purposes, the prototype includes a clinician demo UI for “Moala Health Centre”. Moala oversees the receipt of medicine orders as well as monitoring inventory levels, distributing to patients, and being informed via the supply chain system of any compromised medication batches.

The IoT simulation will be utilized during this demonstration to mimic tracking a temperature-sensitive medication to its destination.

Suppose the temperature rises above the max threshold during transit; the device signs the reading and sends it through the simulated latency path. The edge service verifies the signature, fetches the threshold (from SupplyChainRegistry smart contract), detects the breach, logs the rule violated (“Temperature > maxThreshold”), signs the attestation, and submits an AlertRaised event on the blockchain (ComplianceGuardian). On the UI side, the dashboard shows the alert, the rule reason, the transaction hash, and flags the batch as “Status: ALERT”. The clinician sees in the Dashboard: low-stock items, flagged batches, recent orders, and incoming deliveries. They decide to hold the batch, trigger a recall, or notify the regulator, depending on protocol. The UI also shows latency benchmark results for 4G vs 5G from the simulated benchmark run.

These results agree with previous research, which has established that integrating edge computing with blockchain will improve system responsiveness and reliability.

The proposed architecture improves latency in comparison with traditional cloud-based healthcare supply chain architectures by allowing decision-making at the edge. It allows real-time detection of anomalies before data is put onto the blockchain, whereas blockchain-only architectures only provide an auditable record of data when put on-chain. This hybrid approach improves responsiveness, traceability, and trustworthiness in the process.

5 Scalability Limits and Constraints

The prototype serves as an appropriate proof of concept; however, it has its limitations. First, the blockchain was simulated on a local node (Hardhat) and does not accurately capture the way that distributed consensus mechanisms will operate when deployed in the real world. This includes that there was no measurement of how different levels of network congestion or delay due to node synchronization will affect performance, i.e., there was no consideration of the data throughput limits in conjunction with the rated throughput of the data on the blockchain.

Second, the methodology is currently being laid over an IoT simulated environment, and as such, there will be a change in performance characteristics of the prototype based on the deployment of real devices. This includes unreliable connections between devices, hardware platform limitations, and different types of environmental conditions.

Scalability is another factor that will have to be considered. Classifying scalability with respect to the number of devices will create challenges with data volume, processing capacity at the edge, and transaction costs on the blockchain.

Future work focusing on adapting multi-node blockchain deployments (i.e., Hyperledger Fabric) to support large-scale IoT networks and conduct tests under real-world network conditions.

6 Conclusion

This chapter has developed a complete proof of concept for an intelligent, secure healthcare supply chain that leverages IoT telemetry, edge computing, 5G latency simulation, blockchain smart contracts, and device/edge identity controls, along with explainable anomaly detection. The objective was to explore how ultra-low-latency telemetry (4G vs 5G), on-chain provenance, and two-step alert verification can be used to protect patients from tainted medications through explainable analytics at the edge. The results show significant improvements in latency, high alert accuracy rates, and excellent compliance with regulatory requirements (expiry questions, licensing checks, and zero-trust identity).

The contributions are threefold:

- an architectural blueprint combining 5G/edge/IoT/ blockchain for healthcare supply chains.
- experimental evidence (latency reduction, throughput, alert-detection) showing feasibility.
- a demonstrator UI and scenario (Moala Health Centre) showing how clinicians/inventory managers can leverage the system.

There are still some limitations. The blockchain layer was local and not a full enterprise network. Anomaly detection was rule-based instead of using full AI. Real-world IoT sensors and logistics challenges like connectivity and durability were not fully addressed. Future work will focus on using a permissioned multi-party blockchain such as Hyperledger Fabric, adding machine learning to the anomaly engine, and including formal compliance workflows like automated recall, regulator notification, and RBAC as described in NIST SP 800-207A. Scaling to thousands of devices, multi-region edge nodes, and real cold-chain pharmaceuticals will also be important.

Currently, rule-based anomaly detection relies on transparency and ease of use when it comes to detecting anomalies; however, machine learning-based methods can increase the accuracy of detecting complicated patterns. Unfortunately, machine learning also presents its own set of challenges regarding explainability, processing cost, and conformance to regulations; therefore, the proposed design will prioritize explainability.

Further research will study how combined models can be created that allow for a balance between accurate outputs and explainable ones. In conclusion, this model provides a very good solution for creating healthcare supply chains that are resilient, visible, and fast to react to all the changes happening in global logistics that impact patient safety.

References:

[1] P. De Giovanni, "Blockchain and smart contracts in supply chain management: A game theoretic model," International Journal of Production Economics, Vol. 228, 107855, 2020, doi: 10.1016/j.ijpe.2020.107855.

[2] T. J. Heeres, T. M. Tran, B. A. C. Noort, "Drivers and Barriers to Implementing IoT in the Healthcare Supply Chain: Mixed Methods Multicase Study" Journal of Medical Internet Research, Vol. 25, 2023, doi: 10.2196/48730.

[3] M. Fiore, A. Capodici, P. Rucci, A. Bianconi, G. Longo, M. Ricci, F. Sanmarchi, D. Golinelli, " Blockchain for the Healthcare Supply Chain: A Systematic Literature Review," Applied Sciences vol. 13, no. 2, 686, 2023, doi: 10.3390/app13020686.

[4] A. Rizzardi, S. Sicari, J. F. Cevallos, A. Coen-Porisini, "IoT-driven blockchain to manage the healthcare supply chain and protect medical records" Future Generation Computer Systems, Vol. 141, pp. 563–577, 2024, doi: 10.1016/j.future.2024.07.039.

[5] M.A. Rashid, K. Deo, D. Prasad, K. Singh, S. Chand, M. Assaf, "TEduChain: a blockchain-based platform for crowdfunding tertiary education," The Knowledge Engineering Review. Vol. 35, e27, 2020, doi:10.1017/S0269888920000326.

[6] S. Dhingra, R. Raut, K. Naik, K. Muduli, "Blockchain technology applications in healthcare supply chains: A review," IEEE Access, Vol. 12, pp. 11230-11257, 2024, doi: 10.1109/ACCESS.2023.3348813.

[7] Y. Y. Ghadi, T. Mazhar, T. Shahzad, M. A. Khan, A. Abd-Alrazaq, A. Ahmed, H. Hamam,

"The Role of Blockchain Technology in Securing the Internet of Medical Things" Scientific Reports vol. 14, p. 18422, 2024, doi: 10.1038/s41598-024-68529-x.

[8] Z. Hai, Z. Dongni, Z. Man, Z. Shuanghui, Y. Chao, C. Chunfeng, "The Applications of Internet of Things in Smart Healthcare Sectors: a bibliometric and deep study" Heliyon, vol. 10, no. 3, 2024, doi: 10.1016/j.heliyon.2024.e25392.

[9] M. Oliveira, S. Chauhan, F. Pereira, C. Felgueiras, D. Carvalho, "Blockchain protocols and edge computing targeting Industry 5.0 needs," Sensors, vol. 23, no. 22, p. 9174, 2023, doi: 10.3390/s23229174.

[10] S. K. Nanda, "Medical Supply Chain Integrated with Blockchain and IoT for Tracking the Logistics of Medical Products," Multimedia Tools and Applications vol. 82, p. 32917 – 32939, 2023, doi: 10.1007/s11042-023-14846-8

[11] B. Bhasker, P. Muralidhara Rao, P. Saraswathi, S. Gopal Krishna Patro, J. Khan Bhutto, S. Islam, M. Kareemullah & A. Frinjo Emma , "Blockchain framework with IoT device using federated learning for sustainable healthcare systems," Scientific Reports, vol. 15, p. 26736, 2025, doi: 10.1038/s41598-025-06539-z.

Contribution of Individual Authors to the Crea-tion of a Scientific Article (Ghostwriting Policy)

The conceptualization of the research framework, objectives, and prototype alignment with healthcare compliance standards was developed by SERUWAIA ROKOLATU.

The IoT simulator, edge service, and smart con-tract logic (including latency benchmarking) were developed by SERUWAIA ROKOLATU.

SERUWAIA ROKOLATU created the Type-Script/Express edge service, blockchain contracts, and dashboard user interface.

SERUWAIA ROKOLATU ran simulations to val-idate the model, analysed latency metrics, and assessed the accuracy of anomaly detection.
Statistical comparisons (mean, median, variance, confidence intervals) between 4G and 5G simula-tions were completed by BIBHYA SHARMA.

BIBHYA SHARMA analysed literature and de-termined under-represented areas in research, as well as how the prototype fits into those currently existing research projects.

MANSOUR ASSAF composed the manuscript's first draft (including the introduction, literature review, and experimental methodology).

BIBHYA SHARMA revised the manuscript to create a correctly formatted reference list, ensure that the manuscript complied with journal stand-ards, and compile the final version of the manu-script.

MANSOUR ASSAF created figures 1-3 (system overview, architecture, throughput) and created explainability logs.
The overall programmatic leadership function of MANSOUR ASSAF provided an organization of the collaborative activities and monitoring of the development of the project.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.