International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 5, Sep-Oct 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

NAIBHSC: A Novel Integrated IoT and Blockchain Framework for Secure, Traceable and Efficient Healthcare Supply Chain Management

Pramod Kumar Yadav[*1], Dr.Vivek Kumar[*2]
[*1] Research Scholar, Mahakaushal University, Jabalpur, (M.P.)
[*2]Professor, Mahakaushal University, Jabalpur, (M.P.)

Abstract:
Healthcare supply chains involve many independent stakeholders, from raw-material suppliers and manufacturers to distributors, pharmacies and patients, and they remain vulnerable to counterfeit drugs, loss of product integrity during transport, opaque record keeping and delayed payments. This paper proposes NAIBHSC, a novel approach that integrates the Internet of Things (IoT) with the Ethereum blockchain to provide end-to-end traceability and secure data exchange in the medical supply chain. A bi-objective supply chain network model is formulated to maximize the flow of undamaged products and minimize the total channel cost. The architecture combines RFID tags, QR codes and environmental sensors with Solidity smart contracts that automate product registration, sale authorization, purchase, ownership transfer, invoicing and payment, while an HTTP server, a PostgreSQL database and the InterPlanetary File System (IPFS) handle off-chain data. The prototype was developed with web3j, JSON-RPC and Infura, compiled and tested in Remix IDE, and audited with SmartCheck. A qualitative comparison shows that NAIBHSC provides data decentralization, flexibility, product integrity, security and transparency that are not available in existing non-blockchain approaches, together with off-chain storage and programmable smart contracts that are lacking in existing blockchain-based solutions. Performance benchmarking with Hyperledger Caliper for 100, 300 and 500 concurrent users yielded average query latencies of 145, 162 and 403 ms and minimum latencies of 100, 103 and 110 ms, with throughput scaling to approximately 100 transactions per second for 500 users. The results demonstrate that NAIBHSC improves the security, transparency and responsiveness of healthcare supply chain management.

***Keywords*—**blockchain; Internet of Things; healthcare supply chain; smart contracts; Ethereum; traceability; counterfeit drugs

1. INTRODUCTION

A blockchain is a decentralized, append-only ledger in which transactions are grouped into blocks that are cryptographically linked to their predecessors and replicated across a peer-to-peer network, so that records cannot be altered without consensus of the participants [1]. Smart contracts, programs that execute automatically on the blockchain when predefined conditions are met, extend this ledger into a platform for trusted automation among parties that do not trust one another [2]. Healthcare has been identified as one of the most promising application domains of the technology, with potential uses in medical records, clinical research, insurance and the pharmaceutical supply chain [3]–[6].

Healthcare supply chains are long and fragmented. A single medicine may pass through dozens of roles between the supplier of active ingredients and the patient, and each organization typically keeps its own records in a centralized system. This fragmentation limits visibility, delays the detection of errors, complicates recalls and creates opportunities for counterfeit and substandard products to enter the legitimate channel [7]. Temperature-sensitive products such as vaccines and biologics add a further requirement: their condition must be monitored continuously during transport. The COVID-19 pandemic exposed these weaknesses dramatically, as shortages of vaccines and personal protective equipment were accompanied by fraud and poor traceability.

Blockchain can address several of these problems. Its immutable and shared ledger provides a single source of truth for all participants and supports provenance tracking and anti-counterfeiting [8], [9]. Pilot studies have demonstrated blockchain-based monitoring of pharmaceutical shipments [10] and drug traceability [11]. However, a blockchain alone cannot observe the physical world. The Internet of Things (IoT) supplies this missing link through RFID tags, barcodes, GPS modules and environmental sensors that capture the identity, location and condition of goods in real time [12]. The combination of blockchain and IoT is therefore attractive, but it also raises challenges of scalability, latency, device security and data volume [13]–[15].

To address these challenges, this paper proposes a Novel Approach for Integrated IoT with Blockchain in the Health Supply Chain (NAIBHSC). The main contributions are as follows. First, a bi-objective supply chain network model is formulated that maximizes the quantity of undamaged products delivered and minimizes the total channel cost. Second, a layered architecture is designed in which IoT devices, an Ethereum blockchain, smart contracts and off-chain storage cooperate to track medical products from manufacturer to consumer. Third, smart contract algorithms are developed to automate product registration, sale, purchase and ownership transfer, thereby automating invoicing and payment. Fourth, a working prototype is implemented and compared with existing non-blockchain and blockchain-based approaches, and its response time and latency are benchmarked under increasing user loads.

The remainder of the paper is organized as follows. Section 2 reviews related work. Section 3 presents the network model and the NAIBHSC architecture. Section 4 describes the implementation. Section 5 presents the comparative and performance results, and Section 6 concludes the paper.

2. RELATED WORK

Research on blockchain for supply chains has progressed from conceptual analyses to domain-specific prototypes. Saberi *et al.* [8] analysed how blockchain can support sustainable supply chains and identified inter-organizational, technical and external barriers to adoption, while Kshetri [9] showed how blockchain contributes to cost, quality, speed, dependability, risk reduction and flexibility objectives. In agriculture, Tian [12] combined RFID and blockchain to trace food products from farm to consumer. For pharmaceuticals, Bocek *et al.* [10] described a commercial system in which temperature sensors report shipment conditions to a public blockchain, and Musamih *et al.* [11] proposed Ethereum smart contracts with IPFS to trace drugs and manage recalls. Mackey and Nayyar [7] reviewed digital technologies for combating the global trade in falsified medicines and highlighted the value of serialization and distributed ledgers.

The integration of blockchain with IoT has been examined from a security standpoint. Christidis and Devetsikiotis [2] discussed how smart contracts enable autonomous interactions among IoT devices. Dorri *et al.* [15] proposed a lightweight blockchain architecture for IoT privacy, and Khan and Salah [14] and Reyna *et al.* [13] surveyed the security benefits and open challenges of combining the two technologies, including limited device resources, throughput and storage. Table 1 summarizes representative studies and the gaps addressed by the present work.

Table 1. Summary of representative studies on blockchain-enabled supply chains and IoT integration

Study	Domain	Technologies	Limitation addressed by NAIBHSC
Tian [12]	Agri-food traceability	RFID, blockchain	Not tailored to medical products; no smart-contract payments
Bocek *et al.* [10]	Pharma cold chain	Sensors, public blockchain	Monitoring only; no ownership transfer workflow
Musamih *et al.* [11]	Drug traceability	Ethereum, IPFS	No integrated IoT sensing layer
Dorri *et al.* [15]	Smart-home IoT	Lightweight blockchain	Not a supply chain system
Kshetri [9], Saberi *et al.* [8]	Supply chain management	Conceptual analysis	No implementation or performance evaluation

3. PROPOSED NAIBHSC APPROACH

3.1 Supply Chain Network Model

The healthcare supply chain network considered in this work consists of suppliers $s \in S$, manufacturers $m \in M$, demand (damage or consumption) locations $d \in D$, end users $e \in E$, products $p \in P$, product damage types $j \in J$ and time periods $t \in T$. Key parameters include the quantities shipped from suppliers to manufacturers (QS_{psmt}) and from manufacturers to demand locations (QS'_{pmdt}), the corresponding remaining product lifetimes (LT'_{psmt}, LT_{pmdt}), order quantities (QO), purchase costs (PC), transportation costs (TC), maintenance costs (MC), delay costs (DC) and distances between nodes (F). The model pursues two objectives. The first maximizes the quantity of undamaged products delivered, using an exponential function of the remaining lifetime to express the probability that a product arrives in good condition:

$$\mathrm{MaxUD} = \sum_{m=1}^{M} \sum_{p=1}^{P} \sum_{s=1}^{S} \sum_{t=1}^{T} \left[(1 - e^{-LT'_{psmt}}) QS_{psmt} + (1 - e^{-LT_{pmdt}}) QS'_{pmdt} \right] \tag{1}$$

The second objective minimizes the total channel cost. A weighting factor α balances the cost associated with the distance between damaged locations and end users against the operational costs of transportation, maintenance, delay and purchase:

$$\mathrm{MinTC} = \alpha \sum_{p=1}^{P} \sum_{j=1}^{J} \sum_{e=1}^{E} N_{jde} F_{de} Z_{jde} + (1-\alpha)[C_{\mathrm{transport}} + C_{\mathrm{maintenance}} + C_{\mathrm{delay}} + C_{\mathrm{purchase}}] \tag{2}$$

$$C_{\mathrm{transport}} = \sum_{m,p,s,t} TC_{psmt} QO_{psmt} F'_{ms} + \sum_{d,p,m,t} TC'_{pmdt} QO'_{pdmt} F''_{md}, \qquad C_{\mathrm{purchase}} = \sum_{m,p,s,t} PC_{psmt} QO_{psmt} \tag{3}$$

$$C_{\mathrm{delay}} = \sum_{d,p,m,t} QO''_{pmt} \frac{DC^2_{pmt}}{2QO'_{pdmt}}, \qquad DC_{pmt} = \frac{2QO'_{pdmt}}{T_m} \tag{4}$$

Here, N_{jde} denotes the quantity of damaged items of type j moving from location d to end user e, Z_{jde} is the corresponding decision variable, and T_m is the cycle time at manufacturer m. By maximizing undamaged delivery while minimizing cost, the model captures the dual concern of product quality and efficiency that motivates real-time IoT monitoring and blockchain-based coordination in the proposed approach.

3.2 System Architecture

The NAIBHSC architecture, shown in Fig. 1, consists of a front end, a back end and a set of IoT devices distributed along the supply chain. The front end comprises web and mobile user interfaces through which manufacturers, distributors, pharmacists and customers interact with the system. The back end is built around the Ethereum blockchain, on which smart contracts execute within the Ethereum Virtual Machine, together with an HTTP server and a PostgreSQL database. The logical organization of these components into four layers is illustrated in Fig. 2.

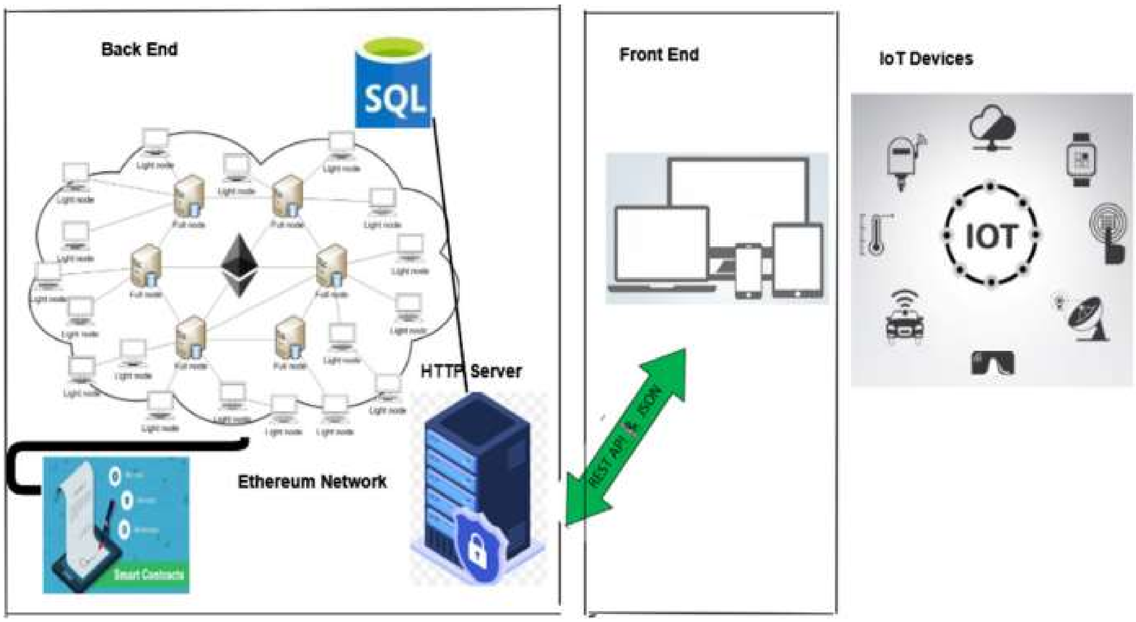

Fig. 1. NAIBHSC framework integrating IoT devices, front-end interfaces, the HTTP server, the database and the Ethereum blockchain network.

The main components are as follows. The Ethereum blockchain network provides open access and verifies the data recorded by participants. Smart contracts define the operations required for access control and product handling; users interact with them through a REST API using JSON messages, and the contracts validate each request before granting rights or executing a transaction. The HTTP server processes queries and connects the front end with the blockchain and the database. The PostgreSQL database stores user information and sensor reports, which are referenced on-chain by URLs, while product images are stored on IPFS [16] and referenced by their content hashes. IoT devices, including RFID tags, barcodes, QR codes, GPS modules, temperature and pressure sensors, and actuators, capture the identity, position and condition of products.

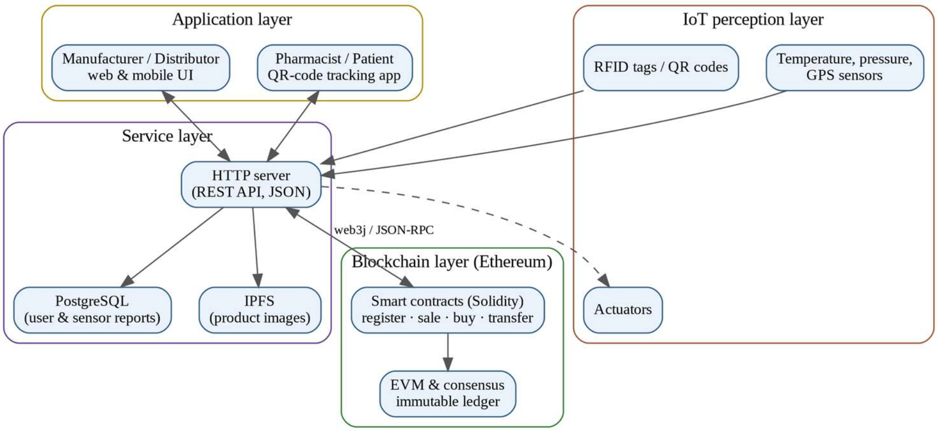

Fig. 2. Layered view of the NAIBHSC architecture showing the IoT perception, blockchain, service and application layers.

3.3 IoT-Enabled Tracking and Monitoring

Before dispatch, the sender associates each consignment with the MAC addresses of its attached sensors and with a QR code that serves as its trace code. During transit, the sensors measure temperature, pressure, sound level, voltage and GPS position. Because the memory of sensor devices is limited, readings are recorded every 10 minutes. The server identifies the product to which each report belongs and forwards the relevant information to the blockchain, where smart contracts continuously compare incoming values with the permitted thresholds. If an anomaly is detected, the smart contract immediately notifies both the product owner and the recipient, and actuators may execute corrective actions, for example adjusting the temperature of a container. On receipt, the customer can download the complete sensor log and submit it to the smart contract for final verification. Sender and recipient can query the status of a product at any time through the API, and scanning the QR code reveals its current location and ownership history. The interactions among participants are summarized in Fig. 3.

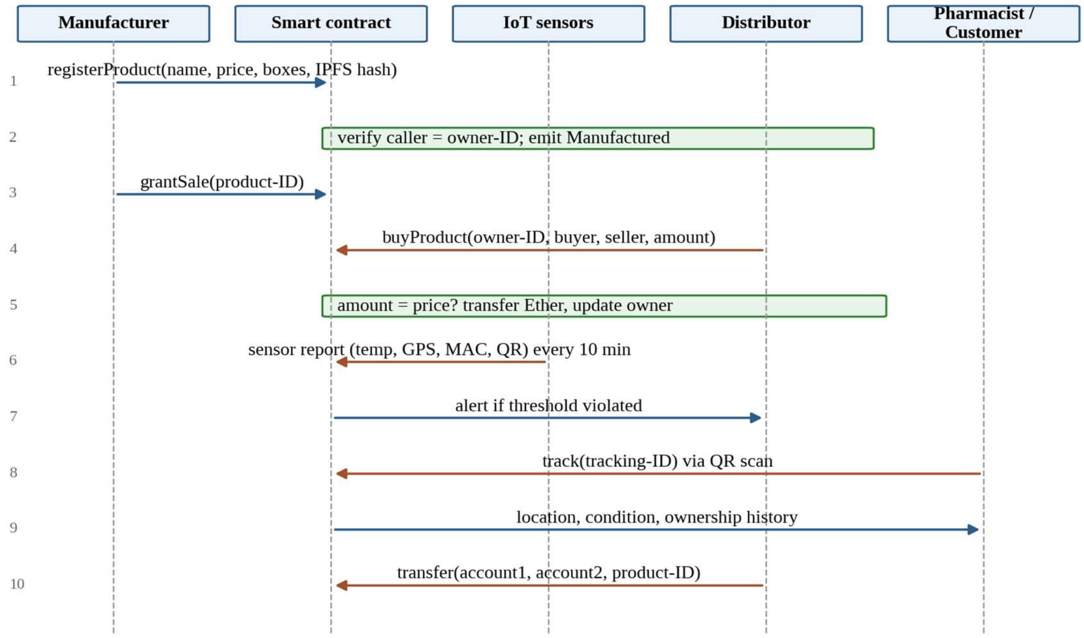

Fig. 3. Sequence of interactions among the manufacturer, smart contract, IoT sensors, distributor and pharmacist/customer in NAIBHSC.

3.4 Smart Contract Algorithms

Three core smart contracts automate the life cycle of a product. Algorithm 1 registers a manufactured product and stores the IPFS hash of its image; only the owner can perform this operation. Algorithm 2 authorizes the sale of the product, and Algorithm 3 executes a purchase by transferring the price to the seller and updating the owner identifier to the buyer's Ethereum address, which automates invoicing and payment. Any violation of the conditions reverts the transaction.

Algorithm 1. Register a manufactured product (shipment contract)

```
Input: product name, product price, number of boxes, price per box, IPFS hash, caller, owner-ID
Output: confirmation that the product has been manufactured and its image uploaded to IPFS
if caller == owner-ID then
    update product name, product price, number of boxes and price per box
    add IPFS hash value of the product image
    emit "Product manufactured" and "Product image uploaded to IPFS"
else
    revert the transaction and generate an error message
```

Algorithm 2. Grant product sale

```
Output: product is ready for sale
if caller == owner-ID then
    mark product as ready for sale
else
    revert the transaction and generate an error message
```


Algorithm 3. Buy product

```
Input: owner-ID, buyer address, seller address, transferred amount, product price
Output: confirmation that the product has been sold
if buyer ≠ seller AND transferred amount == product price then
    transfer the product price to the seller
    owner-ID ← buyer Ethereum address
    emit "Product sold"
else
    revert the transaction and generate an error message
```

3.5 Advantages of the Proposed Approach

NAIBHSC offers several advantages for healthcare supply chain management. Every lot carries a tag that records its movements and interactions, so products can be authenticated and traced back to their original producer, which helps identify and remove counterfeit drugs. Records of producers, regulators, distributors and consumers are preserved immutably, providing transparency and security without relying on a trusted third party. IoT integration provides real-time information to all participants, and blockchain consensus provides fault tolerance by preventing malicious nodes from propagating false data. Finally, smart contracts automate invoicing, payments and delivery confirmation, reducing documentation, human error and opportunities for fraud.

4. IMPLEMENTATION

The prototype was implemented on the Ethereum blockchain using the development environment summarized in Table 2. Smart contracts were written in Solidity and compiled, deployed and tested in the Remix IDE. Interaction between the application and the blockchain was realized through web3j, JSON-RPC and Infura. The SmartCheck static analyser [17] was used to detect vulnerabilities in the contract code, complementing symbolic-execution tools such as Oyente [18].

Table 2. Development environment of the NAIBHSC prototype

Item	Specification
Platform	Ethereum blockchain
Languages	Solidity, HTML, CSS, JavaScript
Operating system	Windows 10, 64-bit
Browsers	Google Chrome, Microsoft Edge, Firefox
Front-end integration	web3j, JSON-RPC, Infura
Test environment	Remix IDE
Security analysis	SmartCheck
Performance benchmarking	Hyperledger Caliper

Each participant in the supply chain is identified by its own Ethereum address (Table 3). Smart contracts use these addresses to authenticate participants and to finalize transactions, so that every action on a product is attributable to a specific stakeholder.

Table 3. Ethereum addresses of the supply chain participants in the prototype

Participant	Ethereum address
Current product owner	0x963865f57804b38459dd4b2da2f760211a200438
Manufacturer	0x99c289eb2aacec289631a5ddf62cf27a63d4494f
Wholesale distributor	0xf1b1bcd24dad92303dd9fe78be639f7bcf9c238d
Retail distributor	0x5d777e9127b28fb119e81a6304278a0a21bef1c4
Pharmacist	0x0fb2bfefd526966c87efa19f6693d50971763fc2

The web application supports four main functions (Fig. 4). In the registration module, a manufacturer must hold an account before registering a product by providing its name, price, specifications and description. In the tracking module, the manufacturer and the customer use the tracking identifier issued before shipment to view the latitude and longitude of the goods. In the transfer module, the parties reach consensus and the smart contract transfers funds from the buyer's account to the seller's account against the product identifier.

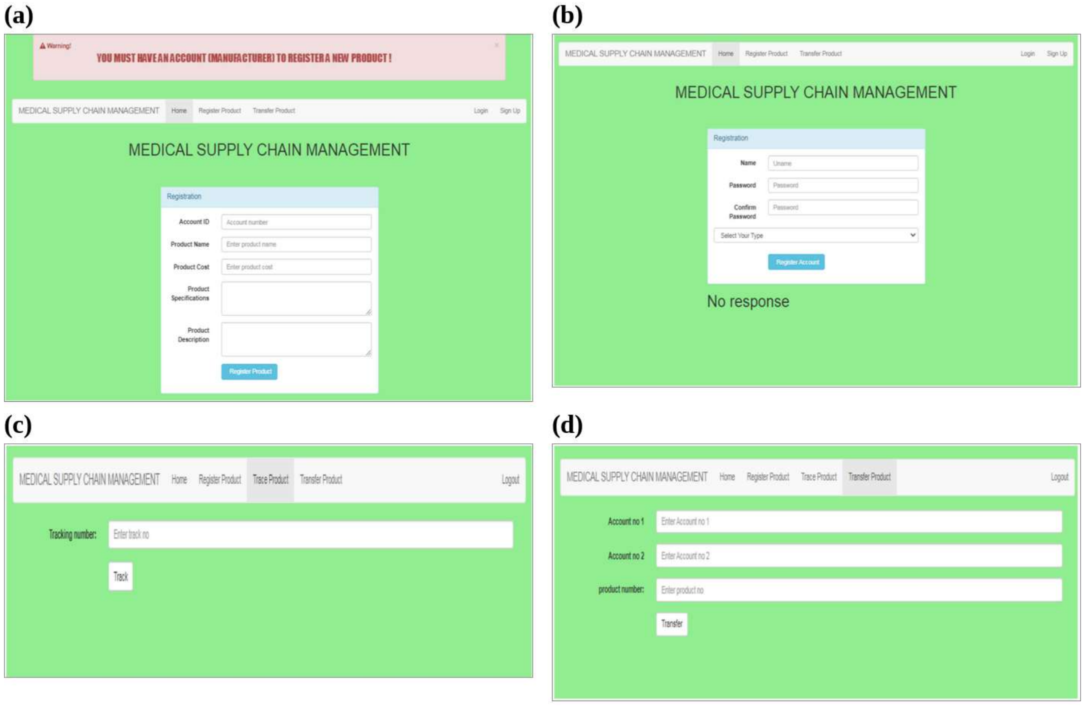

Fig. 4. User interfaces of the NAIBHSC prototype: (a) product owner registration, (b) product registration, (c) product tracking and (d) product transfer between participants.

5. RESULTS AND DISCUSSION

5.1 Comparison with Non-Blockchain Approaches

NAIBHSC was first compared with existing healthcare supply chain approaches that do not use blockchain, namely a smart tracking solution (Kumar), a graph-theory matrix approach (Singh) and a near-field communication approach (Kuandee), as summarized in Table 4. All three existing approaches support tracking and tracing, but none provides data decentralization, flexibility, product integrity, product security or product transparency. Because NAIBHSC stores data on a decentralized ledger, no single entity can be attacked to alter or damage the records, and the use of multiple IoT devices enables more effective tracking and tracing than the existing methods.

Table 4. Comparison of NAIBHSC with existing non-blockchain healthcare supply chain approaches

Feature	Kumar (smart track)	Singh (graph-theory matrix)	Kuandee (NFC)	NAIBHSC
Data decentralization	Not available	Not available	Not available	Available
Flexibility	Not available	Not available	Not available	Available
Product integrity	Not available	Not available	Not available	Available
Tracking and tracing	Available	Available	Available	Available (more effective)
Product security	Not available	Not available	Not available	Available
Product transparency	Not available	Not available	Not available	Available

5.2 Comparison with Blockchain-Based Approaches

NAIBHSC was next compared with existing blockchain-based supply chain solutions built on Bitcoin (Huang), Hyperledger Fabric (Faisal) and the BCTLF framework (Humayun), with respect to platform, permission model, cryptocurrency, off-chain storage and programmability (Table 5). Unlike the Bitcoin-based system, NAIBHSC offers programmable smart contracts rather than a container-based module; unlike the Fabric and BCTLF solutions, it uses a public permission model and a native currency (Ether) for automated payments. NAIBHSC is also the only approach that supports off-chain storage, which is essential because sensor logs and product images are too large to be stored economically on-chain. A consolidated view of the feature comparison is given in Fig. 5.

Table 5. Comparison of NAIBHSC with existing blockchain-based supply chain approaches

Attribute	Huang *et al.*	Faisal *et al.*	Humayun	NAIBHSC
Platform	Bitcoin	Hyperledger Fabric	BCTLF framework	Ethereum
Permission	Public	Private	None	Public
Currency	Bitcoin	None	None	Ether
Off-chain data storage	Not available	Not available	Not available	Available
Programmable module	Docker container	None	None	Smart contracts

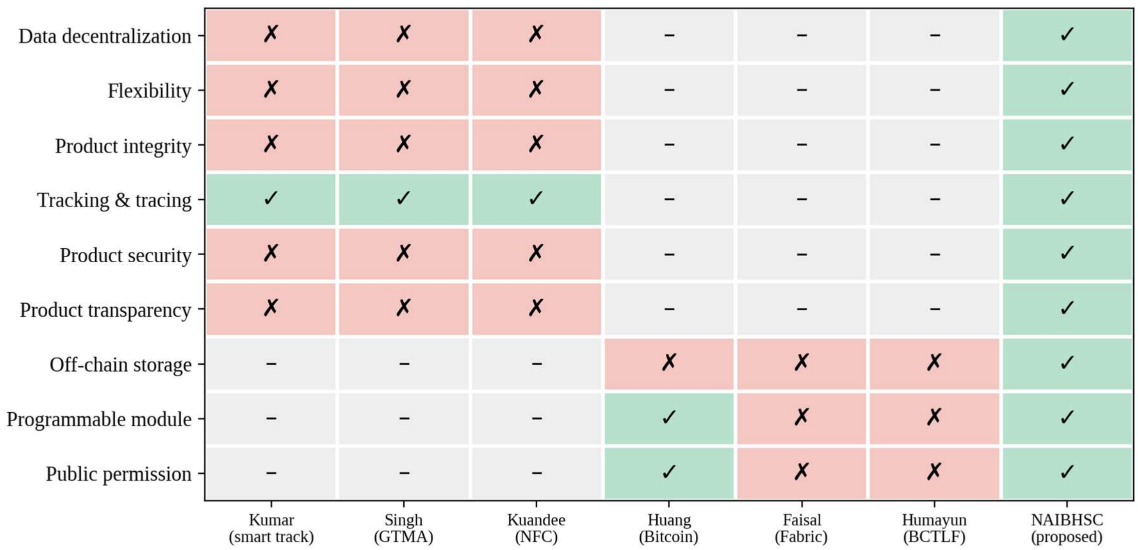

Fig. 5. Feature coverage matrix of NAIBHSC and existing non-blockchain (left) and blockchain-based (right) approaches (✓ available, ✗ not available, – not evaluated).

5.3 Performance Evaluation

Performance was evaluated with Hyperledger Caliper, an open-source benchmarking tool for blockchain systems that measures response time, latency, success rate, throughput and resource consumption. Response time is the total time required to process a request and return a response through the ledger, and latency is the time taken for a network transaction to complete. Three user groups of 100, 300 and 500 simultaneously connected users were tested.

Fig. 6 shows the response times of the three user groups over the test duration. Throughput increased in proportion to the number of users: the average was approximately 70 transactions per second (TPS) for 300 users and 100 TPS for 500 users, with a typical peak of about 115 TPS over the 100 s test period. Response times remained within a stable band for all groups, indicating that the smart contracts handled concurrent requests without saturation.

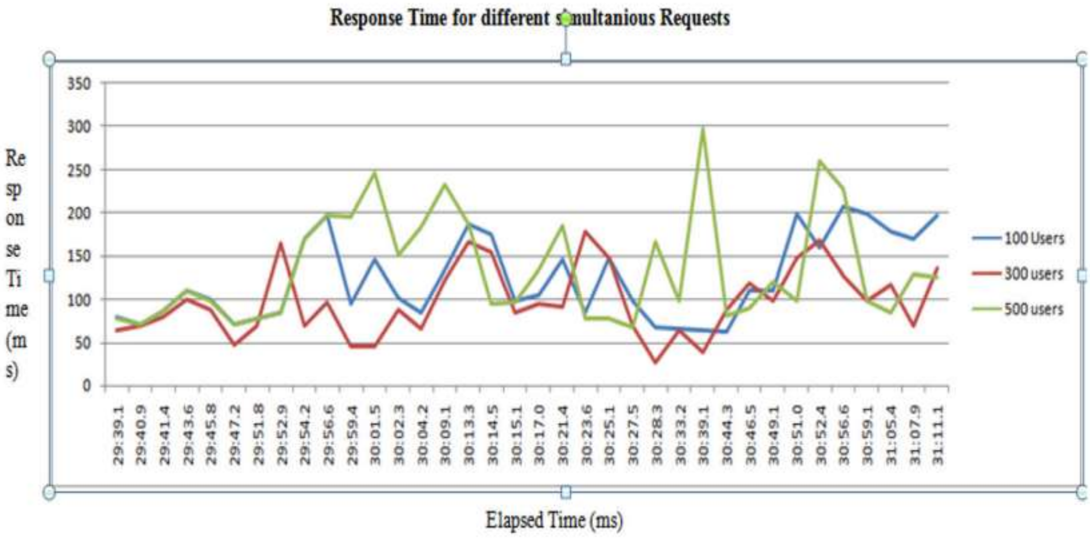

Fig. 6. Response times for 100, 300 and 500 simultaneous requests over the test period.

The latency of the query (GET) transaction is summarized in Table 6 and Fig. 7. Minimum latency was nearly constant at 100, 103 and 110 ms for 100, 300 and 500 users, showing that the intrinsic processing cost of a query is independent of load. Average latency increased only slightly from 145 ms to 162 ms when the load tripled from 100 to 300 users, but rose to 403 ms at 500 users. Tail latencies grew more sharply at the highest load, with the 99th percentile reaching 897 ms and the maximum 1102 ms, compared with 201 ms and 218 ms for 100 users.

Table 6. Latency (ms) of the query transaction for different numbers of concurrent users

Users	Minimum	90% line	95% line	Average	99% line	Maximum
100	100	180	184	145	201	218
300	103	200	209	162	207	434
500	110	703	765	403	897	1102

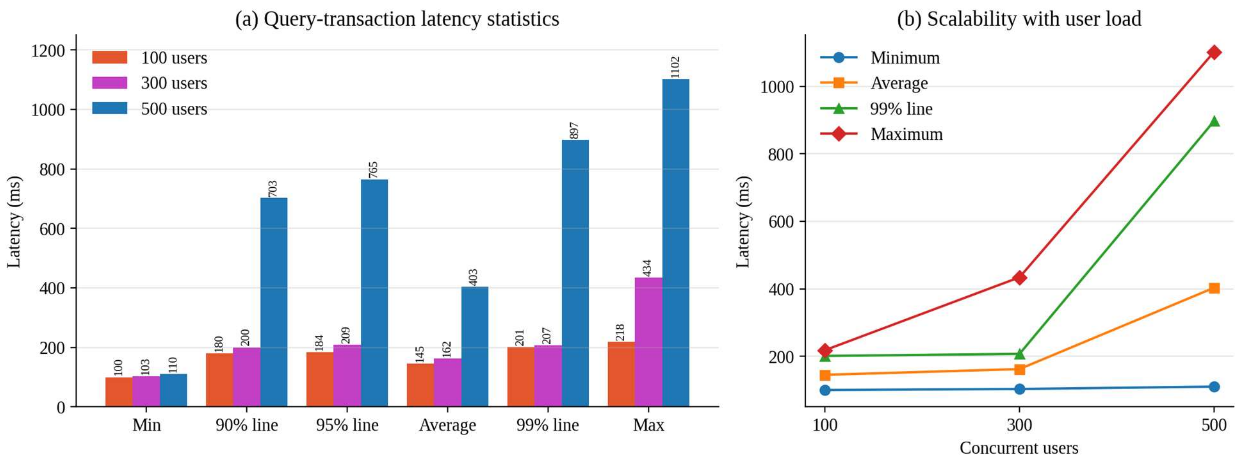

Fig. 7. Query transaction latency: (a) minimum, percentile, average and maximum latency for each user group and (b) growth of latency statistics with increasing user load.

These results show that NAIBHSC maintains sub-second average response for up to 500 concurrent users, which is adequate for supply chain operations such as product registration, tracking queries and ownership transfer, where decisions are made on a time scale of seconds to minutes. The growth in tail latency at 500 users suggests that, for national-scale deployments, techniques such as layer-2 scaling, sharding or a permissioned consortium network could be adopted to further reduce latency [13], [14].

5.4 Discussion

The comparative analysis confirms that the principal value of NAIBHSC lies in the combination of capabilities rather than in any single feature. Blockchain provides decentralization, integrity and transparency that conventional systems lack; IoT provides the real-time physical visibility that blockchain alone cannot offer; and off-chain storage and smart contracts make the approach practical for large sensor data and automated payments. These properties directly support the fight against counterfeit medicines [7] and the monitoring of temperature-sensitive products [10]. Nevertheless, several limitations remain. The use of a public Ethereum network implies transaction fees and exposes metadata, which may be sensitive in commercial supply chains; the security of IoT devices themselves must be ensured because the blockchain cannot correct false sensor readings at the source [14]; and the evaluation was conducted on a prototype with up to 500 users rather than in a live multi-organization deployment.

6. CONCLUSION AND FUTURE WORK

This paper presented NAIBHSC, an integrated IoT and blockchain approach for secure and traceable healthcare supply chain management. A bi-objective network model maximizes undamaged product delivery while minimizing channel cost, and a layered architecture links RFID tags, QR codes and sensors with Ethereum smart contracts, a PostgreSQL database and IPFS. Smart contracts automate product registration, sale, purchase and ownership transfer, including invoicing and payment. Comparisons show that NAIBHSC provides decentralization, flexibility, integrity, security and transparency beyond existing non-blockchain approaches, and off-chain storage and programmability beyond existing blockchain solutions. Benchmarking with Hyperledger Caliper demonstrated average query latencies of 145–403 ms and throughput of about 100 TPS for up to 500 concurrent users. Future work will deploy the system in a consortium setting with real pharmaceutical partners, evaluate energy-efficient consensus mechanisms, integrate machine-learning models for demand forecasting and anomaly detection in sensor data, and assess scalability for thousands of concurrent users.

CONFLICT OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, pp. 557–564, 2017, doi: 10.1109/BigDataCongress.2017.85.

[2] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[3] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *Proc. IEEE 18th Int. Conf. e-Health Netw., Appl. Serv. (Healthcom)*, pp. 1–3, 2016, doi: 10.1109/HealthCom.2016.7749510.

[4] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, Art. no. 470, 2018, doi: 10.3390/sym10100470.

[5] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthcare*, vol. 7, no. 2, Art. no. 56, 2019, doi: 10.3390/healthcare7020056.

[6] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, 2019, doi: 10.1016/j.jnca.2019.02.027.

[7] T. K. Mackey and G. Nayyar, "A review of existing and emerging digital technologies to combat the global trade in fake medicines," *Expert Opin. Drug Saf.*, vol. 16, no. 5, pp. 587–602, 2017, doi: 10.1080/14740338.2017.1313227.

[8] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, 2019, doi: 10.1080/00207543.2018.1533261.

[9] N. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," *Int. J. Inf. Manage.*, vol. 39, pp. 80–89, 2018, doi: 10.1016/j.ijinfomgt.2017.12.005.

[10] 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. Integr. Netw. Serv. Manage. (IM)*, pp. 772–777, 2017, doi: 10.23919/INM.2017.7987376.

[11] 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. 9728–9743, 2021, doi: 10.1109/ACCESS.2021.3049920.

[12] F. Tian, "An agri-food supply chain traceability system for China based on RFID & blockchain technology," in *Proc. 13th Int. Conf. Serv. Syst. Serv. Manage. (ICSSSM)*, pp. 1–6, 2016, doi: 10.1109/ICSSSM.2016.7538424.

[13] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, 2018, doi: 10.1016/j.future.2018.05.046.

[14] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[15] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.

[16] J. Benet, "IPFS—Content addressed, versioned, P2P file system," *arXiv preprint arXiv:1407.3561*, 2014, doi: 10.48550/arXiv.1407.3561.

[17] S. Tikhomirov, E. Voskresenskaya, I. Ivanitskiy, R. Takhaviev, E. Marchenko, and Y. Alexandrov, "SmartCheck: Static analysis of Ethereum smart contracts," in *Proc. 1st Int. Workshop Emerg. Trends Softw. Eng. Blockchain (WETSEB)*, pp. 9–16, 2018, doi: 10.1145/3194113.3194115.

[18] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, pp. 254–269, 2016, doi: 10.1145/2976749.2978309.