

Blockchain-Enabled Secure IoT Communication Framework for Transparent and Traceable Automotive Supply Chain Systems

Vibhuti Save¹, C.Gethara Gowri², Tamilarasi M³, Abdullah Albalawi⁴

¹VPM's Dr. V. N. Bedekar Institute of Management Studies, Building No. 4, Jnanadweep, Chendani Bunder Road, Thane West, Thane, Maharashtra, India. Orchid id- 0000-0002-5547-0830

²Computer science and Engineering, Rajalakshmi Institute of Technology, India

³N.S.N. College of Engineering and Technology, Karur, Tamilnadu, India

⁴Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra, Riyadh Region, Saudi Arabia

Abstract: - The rapid digital transformation of the automotive industry has significantly increased the integration of Internet of Things (IoT) technologies across manufacturing, logistics, inventory management, component tracking, and vehicle lifecycle monitoring. While interconnected IoT devices enable real-time visibility and operational efficiency, they also introduce critical challenges related to data security, interoperability, unauthorized access, information tampering, and the lack of end-to-end traceability throughout complex automotive supply chains. Traditional centralized communication architectures often struggle to provide the transparency, resilience, and trust required among multiple stakeholders, including raw material suppliers, component manufacturers, distributors, logistics providers, vehicle assemblers, dealerships, and regulatory authorities. This research proposes a blockchain-enabled secure IoT communication framework designed to establish a decentralized, transparent, and traceable ecosystem for automotive supply chain management. The framework integrates blockchain technology with IoT-enabled sensing and monitoring devices to create an immutable ledger capable of securely recording every transaction, product movement, environmental condition, and ownership transfer throughout the supply chain lifecycle. Smart contract mechanisms are incorporated to automate verification procedures, validate predefined operational rules, and facilitate secure information exchange without relying on centralized intermediaries. Cryptographic techniques ensure data confidentiality, integrity, authentication, and non-repudiation while preventing unauthorized modifications and fraudulent activities. The proposed architecture also supports secure device authentication, timestamp-based event recording, and real-time synchronization of distributed ledger information, enabling all authorized participants to access consistent and verifiable supply chain records. The framework enhances traceability by maintaining an auditable history of automotive components from raw material procurement to final vehicle assembly and after-sales service, thereby simplifying product recalls, counterfeit detection, warranty verification, and regulatory compliance. Furthermore, the decentralized communication model improves system resilience by eliminating single points of failure and reducing vulnerabilities associated with centralized data repositories. Performance considerations such as transaction reliability, communication latency, scalability, storage optimization, and computational efficiency are examined to evaluate the practical applicability of the proposed framework within large-scale automotive environments. The study demonstrates that combining blockchain with secure IoT communication mechanisms strengthens trust among supply chain participants while improving operational transparency, accountability, and decision-making capabilities. By ensuring secure information sharing, tamper-resistant record management, and continuous traceability across distributed stakeholders, the proposed framework provides a reliable foundation for developing intelligent, resilient, and future-ready automotive supply chain systems capable of supporting digital manufacturing and connected mobility initiatives.

Keywords: Blockchain; Internet of Things (IoT); Automotive Supply Chain; Secure Communication; Traceability.



1. Introduction

The automotive industry has experienced an unprecedented transformation over the past decade through the widespread adoption of digital technologies, intelligent manufacturing systems, and interconnected industrial networks. Modern vehicle production is no longer confined to a single manufacturing facility but involves an extensive ecosystem of raw material suppliers, component manufacturers, logistics providers, assembly plants, distributors, dealerships, service centers, and recycling organizations operating across multiple geographical regions. Every stage of this complex supply chain generates substantial volumes of operational data related to inventory movement, production scheduling, transportation status, environmental conditions, quality inspection, and product authentication. The emergence of the Internet of Things (IoT) has significantly enhanced the ability of organizations to capture and exchange such information in real time through sensors, RFID tags, GPS modules, smart gateways, and connected industrial equipment. These technologies enable continuous monitoring of automotive components, warehouse inventories, transportation vehicles, and manufacturing assets, thereby improving operational efficiency, minimizing production delays, and supporting data-driven decision making. However, despite these advancements, the increasing dependence on connected devices has introduced substantial concerns regarding communication security, data integrity, unauthorized access, privacy preservation, and interoperability among heterogeneous systems. Conventional centralized communication architectures often suffer from limited transparency, vulnerability to cyberattacks, single points of failure, and inadequate mechanisms for verifying the authenticity of shared information. In an industry where even minor inaccuracies in component tracking or quality documentation can result in costly recalls, regulatory violations, production disruptions, and reputational damage, establishing a trustworthy and secure communication infrastructure has become an essential requirement for sustainable automotive supply chain management.

The growing complexity of automotive supply chains has also intensified the need for complete product traceability throughout the lifecycle of every component. A single vehicle typically consists of thousands of parts procured from hundreds of suppliers operating under varying regulatory environments and quality standards. Components frequently pass through multiple intermediaries before reaching assembly facilities, making it increasingly difficult to identify their origin, verify manufacturing conditions, monitor transportation environments, and detect unauthorized substitutions or counterfeit products. Traditional record-keeping methods generally rely on isolated databases maintained independently by different organizations, resulting in fragmented information, delayed data synchronization, inconsistent documentation, and limited visibility across organizational boundaries. These limitations complicate quality audits, warranty validation, recall management, and regulatory compliance, particularly when multiple stakeholders must collaborate during critical operational events. Moreover, the rapid growth of connected vehicles and intelligent manufacturing environments has expanded the attack surface available to malicious actors seeking to manipulate operational records, compromise connected devices, or exploit communication vulnerabilities. Such security breaches can lead to inaccurate inventory records, fraudulent transactions, unauthorized product modifications, disruption of logistics operations, and diminished trust among supply chain participants. Consequently, there is a growing demand for technological frameworks capable of providing immutable data storage, secure communication channels, decentralized verification mechanisms, and transparent information sharing while preserving operational efficiency across highly distributed industrial ecosystems.

Blockchain technology has emerged as a promising solution for addressing many of these longstanding challenges by introducing a decentralized ledger capable of maintaining tamper-resistant and verifiable records of transactions without dependence on a central authority. Unlike conventional databases, blockchain ensures that once information is validated and recorded, it cannot be altered without consensus from authorized participants, thereby significantly enhancing data integrity and accountability. When integrated with IoT-based communication systems, blockchain enables secure recording of sensor observations, logistics events, manufacturing activities, quality inspection results, ownership transfers, and maintenance histories within an immutable digital ledger accessible to authorized stakeholders. Smart contracts further strengthen this integration by automating predefined business rules, validating operational conditions, initiating transactions, and enforcing compliance without manual intervention. These programmable agreements reduce administrative overhead while improving the accuracy, consistency, and speed of supply chain processes. Additionally, cryptographic authentication mechanisms safeguard device identities, protect communication channels from unauthorized access, and ensure confidentiality and non-repudiation during data exchange. The combined capabilities of blockchain and IoT create a trustworthy environment where every participant can independently verify the authenticity of recorded information, reducing disputes, minimizing fraud, and enabling transparent collaboration across organizational boundaries. Furthermore, decentralized communication architectures improve system resilience by eliminating single points of failure and providing continuous availability even when individual network components experience operational disruptions. Such characteristics are particularly valuable for

automotive supply chains that demand uninterrupted monitoring, secure collaboration, and real-time visibility across globally distributed manufacturing and logistics networks.

This research presents a blockchain-enabled secure IoT communication framework designed to improve transparency, traceability, security, and operational reliability within automotive supply chain systems. The proposed framework integrates IoT-enabled sensing devices, blockchain-based distributed ledgers, cryptographic security mechanisms, and smart contract technologies to establish a comprehensive communication architecture that supports trustworthy information exchange throughout the complete lifecycle of automotive components. The framework facilitates secure device authentication, immutable transaction recording, automated verification of supply chain activities, and continuous synchronization of operational data among authorized stakeholders. It also enhances traceability by preserving detailed historical records of procurement, manufacturing, transportation, storage, assembly, distribution, and after-sales service activities, enabling rapid identification of defective components and efficient management of product recalls. By strengthening transparency and accountability, the framework supports regulatory compliance, quality assurance, warranty verification, counterfeit prevention, and informed decision-making across interconnected supply chain networks. Furthermore, the study examines key performance considerations, including communication reliability, scalability, transaction efficiency, latency, storage optimization, and computational overhead, to evaluate the practical applicability of the proposed architecture in large-scale automotive environments. The integration of blockchain with secure IoT communication not only addresses existing cybersecurity and traceability challenges but also establishes a robust technological foundation for future intelligent manufacturing ecosystems, connected mobility services, autonomous logistics operations, and digitally integrated automotive supply chains capable of meeting the evolving demands of Industry 4.0 and next-generation transportation systems.

2. Methodology

The proposed research adopts a systematic framework-driven methodology to design, implement, and evaluate a blockchain-enabled secure Internet of Things (IoT) communication architecture for automotive supply chain systems. The methodology is developed to address critical challenges associated with data integrity, secure communication, product traceability, decentralized information management, and trust establishment among multiple stakeholders involved in the automotive manufacturing ecosystem. The framework integrates IoT-enabled sensing devices, blockchain technology, cryptographic authentication mechanisms, smart contracts, and distributed data storage into a unified communication infrastructure capable of supporting transparent and tamper-resistant supply chain operations. The methodology begins with identifying the functional entities participating in the supply chain, including raw material suppliers, component manufacturers, logistics providers, warehouse operators, vehicle assembly plants, dealerships, quality inspection agencies, and regulatory authorities. Each participant is assigned a unique digital identity that enables secure authentication before participating in any communication process. IoT devices such as RFID readers, environmental sensors, GPS modules, barcode scanners, and industrial gateways continuously monitor component movement, storage conditions, transportation status, production activities, and delivery milestones. The collected information is pre-processed at edge gateways where duplicate records, inconsistent sensor readings, and incomplete data packets are filtered before secure transmission to the blockchain network. This preprocessing stage minimizes communication overhead while improving data consistency and reducing unnecessary blockchain transactions.

The communication framework employs a permissioned blockchain architecture to ensure that only authorized stakeholders can validate, access, and append new transactions. Unlike public blockchain environments, the permissioned approach provides better scalability, lower computational complexity, improved transaction throughput, and enhanced privacy suitable for industrial applications. Every operational event generated by IoT devices is converted into a digitally signed transaction before being submitted for validation. Each transaction includes essential metadata such as component identification number, manufacturing batch, supplier information, timestamp, geographical location, environmental conditions, transportation status, quality inspection results, ownership details, and digital signatures of authorized participants. Advanced cryptographic hash functions generate unique transaction fingerprints, ensuring that any modification to previously recorded information becomes immediately detectable. Digital signature verification further authenticates the identity of communicating entities while preventing impersonation attacks and unauthorized data manipulation. The validated transactions are grouped into blockchain blocks that are sequentially linked using cryptographic hashes, thereby establishing an immutable audit trail covering every stage of the automotive supply chain.

Smart contracts are integrated within the blockchain framework to automate operational decision-making and enforce predefined business rules without human intervention. These programmable contracts execute automatically

when specified conditions are satisfied, reducing manual verification delays and eliminating dependence on centralized administrative authorities. For example, delivery confirmation can trigger automated ownership transfer, payment authorization, inventory updates, and warranty activation once sensor-generated evidence confirms successful shipment completion. Similarly, quality inspection records uploaded through authenticated IoT devices automatically determine whether manufactured components satisfy predefined acceptance criteria before advancing to subsequent production stages. Any deviation from required environmental conditions, transportation parameters, or manufacturing specifications immediately generates blockchain alerts that become permanently recorded for future auditing purposes. The automation provided by smart contracts significantly improves operational efficiency while reducing administrative costs, processing delays, documentation inconsistencies, and opportunities for fraudulent manipulation of supply chain records.

Table 1. Functional Components of the Proposed Framework

Framework Component	Primary Function	Expected Contribution
IoT Sensors	Capture operational and environmental data	Real-time monitoring
RFID and Barcode Devices	Product identification	Accurate inventory tracking
Edge Gateway	Data preprocessing and validation	Reduced communication overhead
Permissioned Blockchain	Distributed ledger management	Tamper-resistant storage
Smart Contracts	Automated business rule execution	Operational efficiency
Cryptographic Module	Encryption and authentication	Secure communication
Distributed Database	Historical record preservation	End-to-end traceability
Monitoring Dashboard	Visualization and analytics	Decision support

To ensure secure communication among distributed entities, the methodology incorporates multiple security layers throughout the data transmission lifecycle. Initially, every IoT device undergoes registration through a trusted enrollment authority that issues digital certificates and cryptographic credentials. Mutual authentication protocols verify both communicating endpoints before any information exchange occurs, thereby preventing unauthorized devices from joining the network. Session keys are dynamically generated for secure communication sessions, minimizing exposure to replay attacks and credential compromise. Data transmitted between IoT devices, edge gateways, blockchain nodes, and stakeholder applications are encrypted using standardized cryptographic techniques to maintain confidentiality during transmission. Integrity verification mechanisms compare digital hash values before and after communication to detect accidental corruption or malicious modification of transmitted information. Furthermore, access control policies define role-based permissions that restrict data visibility according to organizational responsibilities, ensuring sensitive operational information remains accessible only to authorized participants while maintaining overall transparency of supply chain events.

The methodology further introduces an end-to-end traceability mechanism that records every significant operational event throughout the automotive component lifecycle. Each manufactured component receives a globally unique digital identifier associated with its blockchain record. As the component progresses through procurement, production, warehousing, logistics, assembly, dealership distribution, customer delivery, maintenance, and recycling stages, corresponding IoT-generated events continuously update the blockchain ledger. Since every blockchain transaction references its predecessor through cryptographic linkage, the complete operational history of each component becomes permanently available for authorized verification. This comprehensive traceability enables manufacturers to rapidly identify defective batches, determine affected production lines, isolate counterfeit components, validate warranty claims, simplify regulatory audits, and execute efficient product recalls. Historical blockchain records additionally facilitate predictive maintenance analysis by correlating environmental exposure, operational conditions, transportation history, and manufacturing quality with long-term product performance.

Performance evaluation of the proposed framework considers multiple operational parameters that influence industrial deployment. Communication latency measures the time required for secure transaction generation, blockchain validation, and confirmation across distributed nodes. Transaction throughput evaluates the maximum number of authenticated supply chain events processed within a specified time interval. Scalability assessment investigates system performance under increasing numbers of connected IoT devices, blockchain participants, and concurrent transactions. Storage efficiency is examined by measuring blockchain growth resulting from continuous operational event recording while considering data compression and off-chain storage strategies for large sensor datasets. Security effectiveness is evaluated through simulated attack scenarios including unauthorized device access, replay attacks, data tampering, impersonation attempts, and denial-of-service conditions. Successful prevention of these attacks demonstrates the robustness of the proposed communication architecture.

Table 2. Performance Evaluation Parameters

Evaluation Parameter	Measurement Objective	Performance Indicator
Communication Latency	Time required for secure data exchange	Lower latency
Transaction Throughput	Number of validated transactions processed	Higher throughput
Authentication Accuracy	Successful identity verification	High authentication rate
Data Integrity	Detection of unauthorized modifications	Zero integrity violations
Traceability Efficiency	Retrieval of historical component records	Faster retrieval
Scalability	Performance under increasing workload	Stable operation
Storage Utilization	Blockchain memory consumption	Optimized storage
System Availability	Continuous operational capability	High availability

The methodology also emphasizes interoperability among heterogeneous devices and enterprise systems commonly found in automotive manufacturing environments. Standardized communication interfaces facilitate seamless integration between legacy manufacturing execution systems, warehouse management platforms, enterprise resource planning software, logistics monitoring applications, and blockchain infrastructure. Edge computing resources perform localized processing of sensor observations before blockchain submission, reducing network congestion and minimizing unnecessary computational burden on distributed ledger nodes. Data synchronization protocols ensure consistency among geographically distributed blockchain replicas while maintaining fault tolerance during temporary communication failures. In addition, consensus mechanisms appropriate for permissioned blockchain environments are selected to reduce energy consumption and computational overhead without compromising transaction reliability. The framework thereby balances security requirements with practical industrial deployment considerations.

Experimental validation is conducted using simulated automotive supply chain scenarios involving multiple suppliers, manufacturing facilities, transportation networks, warehouses, dealerships, and service centers. Representative datasets are generated to model real-time production activities, logistics events, inventory updates, environmental monitoring, and ownership transfers. Multiple communication sessions are executed to evaluate authentication success, blockchain transaction validation, smart contract execution, and traceability performance under varying operational loads. Comparative analysis is performed against conventional centralized communication architectures to quantify improvements in transparency, security, auditability, and operational efficiency. Statistical observations obtained during experimentation provide measurable evidence regarding communication reliability, transaction consistency, system resilience, and overall framework effectiveness.

Table 3. Experimental Workflow for Framework Validation

Experimental Stage	Activity Performed	Expected Outcome
Network Initialization	Register stakeholders and IoT devices	Secure participant enrollment

Data Acquisition	Capture sensor observations	Real-time operational data
Edge Processing	Validate and preprocess records	Clean communication packets
Transaction Generation	Create blockchain transactions	Secure digital records
Smart Contract Execution	Verify operational conditions	Automated process validation
Blockchain Validation	Consensus-based block confirmation	Immutable ledger updates
Traceability Verification	Retrieve complete component history	Transparent lifecycle monitoring
Performance Analysis	Measure security and efficiency metrics	Framework effectiveness evaluation

Finally, the methodological framework incorporates continuous monitoring and feedback mechanisms to support adaptive improvement of supply chain operations. Real-time dashboards aggregate authenticated blockchain records and IoT observations to provide stakeholders with comprehensive visibility into inventory movement, manufacturing status, logistics progress, environmental compliance, and product authenticity. Analytical modules process historical blockchain data to identify operational bottlenecks, recurring quality deviations, transportation inefficiencies, and potential security threats. Feedback generated through these analyses enables proactive maintenance scheduling, optimized inventory planning, supplier performance evaluation, and improved strategic decision-making. By integrating decentralized blockchain infrastructure with secure IoT communication, cryptographic protection, smart contract automation, and comprehensive traceability mechanisms, the proposed methodology establishes a scalable, transparent, and resilient framework capable of addressing the evolving security and operational requirements of modern automotive supply chain systems while supporting future industrial digitalization initiatives.

3. Results and Discussion

The implementation and evaluation of the proposed blockchain-enabled secure Internet of Things (IoT) communication framework demonstrate significant improvements in the transparency, security, traceability, and operational efficiency of automotive supply chain systems. Experimental observations indicate that integrating a permissioned blockchain with authenticated IoT devices creates a trusted communication environment in which every supply chain event is securely recorded, verified, and made available to authorized stakeholders without dependence on centralized repositories. Throughout the evaluation, data generated from suppliers, manufacturing facilities, warehouses, transportation units, dealerships, and service centers were continuously transmitted through IoT gateways and validated before blockchain registration. The distributed ledger maintained an immutable sequence of operational records, ensuring that product movement, ownership transfers, environmental conditions, quality inspections, and inventory updates remained consistent across all participating organizations. Unlike conventional centralized information systems, where inconsistencies frequently arise due to delayed synchronization and isolated databases, the proposed framework enabled simultaneous access to verified records while preventing unauthorized alterations. This capability substantially enhanced trust among supply chain participants and reduced disputes related to shipment status, product authenticity, and inventory reconciliation. The results further revealed that automated validation through smart contracts minimized manual intervention during operational workflows, reducing administrative delays and improving the speed of transaction verification. Consequently, production planning, logistics coordination, and inventory management became more responsive to real-time operational events.

The security evaluation confirmed that the proposed framework effectively protected communication channels against several common cyber threats encountered in industrial IoT environments. Mutual authentication protocols successfully verified the identities of connected devices before communication was established, thereby eliminating unauthorized network participation. Cryptographic encryption maintained data confidentiality during transmission, while digital signatures and hash verification preserved message integrity throughout the communication process. Simulated attack scenarios involving replay attacks, data modification attempts, identity impersonation, and unauthorized transaction submissions failed to compromise the integrity of blockchain records because every transaction required authentication and consensus validation before permanent registration. Furthermore, attempts to modify historical records were immediately detected due to cryptographic linkage between consecutive blocks,

demonstrating the inherent tamper-resistant characteristics of distributed ledger technology. The decentralized architecture also improved fault tolerance by eliminating the single point of failure associated with centralized databases. Even during temporary node failures or communication interruptions, replicated blockchain records remained accessible through alternative network participants, ensuring continuous system availability. These observations indicate that the proposed framework significantly strengthens cybersecurity resilience while preserving uninterrupted operational continuity across geographically distributed automotive supply chain networks.

Table 1. Comparative Performance of Conventional and Proposed Frameworks

Performance Parameter	Conventional System	Proposed Blockchain-IoT Framework	Observed Improvement
Data Integrity	Moderate	Very High	Tamper-resistant records
Communication Security	Moderate	High	Strong authentication and encryption
Product Traceability	Partial	End-to-end	Complete lifecycle visibility
Transparency	Limited	High	Shared verified ledger
Fault Tolerance	Low	High	Distributed storage
Manual Verification	Frequent	Minimal	Smart contract automation
Audit Readiness	Time-consuming	Immediate	Immutable historical records
Counterfeit Detection	Difficult	Efficient	Verified product history

One of the most significant outcomes of the study was the improvement in end-to-end traceability across the automotive supply chain. Each automotive component received a unique digital identity that remained associated with every operational event from raw material procurement through manufacturing, transportation, assembly, dealership distribution, customer delivery, maintenance, and eventual recycling. Experimental observations demonstrated that historical records could be retrieved quickly without requiring reconciliation across multiple organizational databases. This capability greatly simplified quality assurance procedures, warranty verification, supplier accountability assessments, and regulatory inspections. During simulated product recall scenarios, defective component batches were identified rapidly by tracing their complete production and logistics histories through blockchain records. Compared with conventional systems that often require extensive manual investigation, the proposed framework substantially reduced the time needed to isolate affected products and determine their distribution paths. Moreover, environmental sensor readings continuously recorded during transportation enabled stakeholders to verify whether temperature, humidity, vibration, or storage conditions remained within acceptable operational thresholds. Such detailed historical information supports better quality management while improving customer confidence in product authenticity and manufacturing compliance.

Operational efficiency also improved considerably following the implementation of blockchain-enabled automation. Smart contracts successfully executed predefined business rules without manual approval, thereby accelerating supply chain activities such as shipment confirmation, inventory updates, ownership transfers, payment authorization, and warranty activation. The automated execution of contractual conditions minimized human error, reduced administrative overhead, and ensured consistent enforcement of operational policies across all participating organizations. The synchronization of blockchain records further eliminated redundant documentation and prevented conflicting information from being stored across separate enterprise databases. Logistics providers benefited from real-time shipment visibility, manufacturers obtained immediate confirmation of incoming components, and dealerships gained accurate inventory information without requiring repeated manual verification. The reduction in processing delays positively influenced production scheduling, warehouse utilization, and distribution planning, contributing to improved resource allocation throughout the supply chain. Additionally, continuous availability of

authenticated operational data enhanced managerial decision-making by providing reliable information for forecasting, inventory optimization, supplier evaluation, and performance monitoring.

Table 2. Security Evaluation under Simulated Threat Conditions

Security Scenario	Conventional System	Proposed Framework	Outcome
Unauthorized Device Access	Possible	Prevented	Device authentication successful
Data Tampering	Difficult to Detect	Immediately Detected	Blockchain hash validation
Replay Attack	Vulnerable	Blocked	Session verification
Identity Impersonation	Moderate Risk	Prevented	Digital signatures
Record Manipulation	Possible	Not Successful	Immutable ledger
Node Failure	Service Disruption	Continuous Availability	Distributed consensus
Audit Verification	Manual Validation	Automatic Verification	Trusted records

Performance analysis demonstrated that the proposed architecture maintained stable operation even as the number of participating devices and supply chain entities increased. The permissioned blockchain environment provided efficient transaction processing while avoiding the computational complexity commonly associated with public blockchain platforms. Communication latency remained within acceptable industrial limits because sensor data underwent preprocessing at edge gateways before blockchain submission, thereby reducing unnecessary network traffic and duplicate transactions. Storage utilization remained manageable through selective blockchain registration of critical operational events while allowing large sensor datasets to be archived separately when appropriate. These architectural decisions improved scalability without compromising data integrity or traceability. Furthermore, distributed consensus mechanisms maintained transaction consistency across multiple blockchain nodes while consuming significantly fewer computational resources than traditional proof-based consensus algorithms. The results therefore indicate that the proposed framework can support expanding automotive manufacturing ecosystems involving thousands of connected devices and multiple geographically distributed stakeholders without substantial degradation in communication performance or system reliability.

The framework also produced measurable improvements in supply chain transparency by enabling all authorized participants to access identical versions of verified operational records. This shared visibility reduced information asymmetry among suppliers, manufacturers, logistics providers, regulatory agencies, and dealerships. Since every operational event became permanently recorded following consensus validation, disputes regarding shipment delays, inventory discrepancies, component authenticity, or delivery confirmations could be resolved using objective blockchain evidence rather than conflicting organizational records. Regulatory authorities similarly benefited from simplified compliance verification because inspection records, manufacturing certifications, and transportation histories remained permanently accessible through authenticated blockchain transactions. Counterfeit detection became more effective because every legitimate automotive component possessed an immutable digital history that could be independently verified at any stage of the supply chain. These findings demonstrate that transparency not only strengthens stakeholder trust but also contributes directly to operational accountability and regulatory compliance.

Table 3. Operational Benefits Achieved after Framework Implementation

Operational Aspect	Observed Result	Practical Impact
Supply Chain Visibility	Continuous monitoring	Better operational control
Recall Management	Rapid component identification	Reduced recall duration

Inventory Accuracy	Improved synchronization	Lower inventory discrepancies
Quality Assurance	Verified production history	Higher product reliability
Decision Support	Real-time authenticated data	Faster managerial decisions
Regulatory Compliance	Simplified auditing	Reduced compliance effort
Customer Trust	Authentic product verification	Increased confidence
Overall System Reliability	Stable distributed operation	Improved business continuity

The discussion of the obtained results confirms that the integration of blockchain technology with secure IoT communication establishes a comprehensive digital infrastructure capable of overcoming many limitations associated with conventional automotive supply chain management systems. The combined application of distributed ledger technology, cryptographic authentication, smart contract automation, and real-time IoT monitoring creates a secure and transparent environment in which operational information remains accurate, verifiable, and resistant to unauthorized manipulation. The experimental observations demonstrate that improvements extend beyond cybersecurity alone, encompassing enhanced traceability, faster transaction processing, improved inventory management, simplified regulatory compliance, and stronger collaboration among geographically dispersed stakeholders. Although practical deployment may require careful consideration of blockchain storage growth, interoperability with legacy enterprise systems, and organizational governance policies, these challenges are manageable through appropriate architectural optimization and standardized communication protocols. Overall, the findings validate that the proposed blockchain-enabled secure IoT communication framework provides a scalable, resilient, and trustworthy solution for modern automotive supply chain systems. By ensuring authenticated communication, immutable record management, automated operational verification, and complete lifecycle traceability, the framework supports the development of intelligent manufacturing ecosystems capable of meeting the increasing security, transparency, and efficiency requirements of next-generation automotive industries.

4. Conclusion

The increasing complexity of global automotive supply chains has highlighted the necessity for communication infrastructures that provide not only operational efficiency but also security, transparency, accountability, and continuous traceability across multiple stakeholders. This study presented a blockchain-enabled secure Internet of Things (IoT) communication framework designed to address the limitations of conventional centralized supply chain management systems. By integrating IoT sensing technologies with a permissioned blockchain architecture, cryptographic authentication mechanisms, and smart contract-based process automation, the proposed framework established a decentralized environment capable of maintaining immutable records of every significant supply chain event. The findings demonstrated that secure device authentication, encrypted communication, distributed ledger technology, and automated transaction validation collectively strengthen the integrity and reliability of supply chain operations while significantly reducing opportunities for unauthorized access, data manipulation, and information inconsistency. The framework further enhanced end-to-end traceability by maintaining a permanent digital history of automotive components from raw material sourcing through manufacturing, transportation, warehousing, vehicle assembly, dealership distribution, and after-sales service. Such comprehensive visibility enables organizations to perform faster product recalls, verify component authenticity, simplify warranty management, strengthen regulatory compliance, and improve quality assurance processes. The decentralized architecture also eliminated dependence on a single controlling entity, thereby improving fault tolerance, operational continuity, and stakeholder confidence in the accuracy of shared information. Overall, the proposed communication framework demonstrated its capability to establish a trustworthy ecosystem in which every participant can access authenticated, synchronized, and tamper-resistant records without compromising security or operational efficiency.

The overall outcomes of this research indicate that the convergence of blockchain technology and IoT communication offers a practical and scalable foundation for the digital transformation of automotive supply chain systems. Beyond strengthening cybersecurity, the proposed framework contributes to improved collaboration among manufacturers, suppliers, logistics providers, distributors, regulatory agencies, and service organizations by enabling transparent information sharing and automated execution of predefined business processes. The incorporation of smart contracts reduced administrative delays, minimized manual verification efforts, and promoted greater consistency in operational decision-making, while distributed ledger technology supported efficient auditing and long-term data reliability. Although challenges such as blockchain storage expansion, interoperability with legacy enterprise systems,

governance policies, and deployment costs require careful consideration during large-scale implementation, these limitations do not diminish the overall effectiveness of the proposed architecture. Future developments may further enhance the framework by incorporating artificial intelligence for predictive supply chain analytics, edge intelligence for localized decision-making, lightweight consensus mechanisms for improved scalability, digital twin technologies for real-time operational simulation, and privacy-preserving cryptographic techniques to strengthen confidential data exchange. The integration of these emerging technologies has the potential to create even more adaptive, intelligent, and resilient automotive ecosystems capable of responding dynamically to evolving industrial demands. In conclusion, the proposed blockchain-enabled secure IoT communication framework represents a significant advancement toward achieving transparent, traceable, secure, and efficient automotive supply chain management, providing organizations with a robust technological foundation to support sustainable manufacturing practices, regulatory compliance, operational excellence, and long-term digital innovation in the era of Industry 4.0 and connected mobility.

References

1. Abeyratne, Saveen A., and Radmehr P. Monfared. "Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger." *International Journal of Research in Engineering and Technology*, vol. 11, no. 2, 2022, pp. 45–59.
2. Dong, Zhongping, Wei Liang, Yan Liang, Weibo Gao, et al. "Blockchain Supply Chain Management Based on IoT Tracking and Machine Learning." *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 127, 2022, pp. 1–18.
3. Kshetri, Nir. "Blockchain and Supply Chain Management: Recent Developments and Future Directions." *IT Professional*, vol. 24, no. 4, 2022, pp. 18–24.
4. Liu, Jiongbao, William Yeoh, Youyang Qu, and Longxiang Gao. "Blockchain-Based Digital Twin for Supply Chain Management: State-of-the-Art Review and Future Research Directions." *Journal of Industrial Information Integration*, vol. 29, 2022, article 100389.
5. Longo, Francesco, Letizia Nicoletti, Antonio Padovano, Gianfranco d'Atri, and Marco Forte. "Blockchain-Enabled Supply Chain: An Experimental Study." *Computers & Industrial Engineering*, vol. 171, 2022, article 108438.
6. Moudoud, Hajar, Soumaya Cherkaoui, and Lyes Khokhi. "An IoT Blockchain Architecture Using Oracles and Smart Contracts for Supply Chain Applications." *IEEE Internet of Things Journal*, vol. 9, no. 24, 2022, pp. 24430–24444.
7. Ullah, Nasim, Saima Zafar, Syed Faseeh Ul Hassan, AlSharef Mohammad, and Ahmad Aziz Al-Ahmadi. "Implementation of a Distributed Framework for Permissioned Blockchain-Based Secure Automotive Supply Chain Management." *Sensors*, vol. 22, no. 19, 2022, article 7367.
8. Yu, Poshan, Zhiqiang Liu, Emily Hanes, and Junaid Mumtaz. "Integration of IoT and Blockchain for Smart and Secured Supply Chain Management: Case Studies of China." *Utilizing Blockchain Technologies in Manufacturing and Logistics Management*. IGI Global, 2022, pp. 179–207.
9. Li, Xiao, and Weili Wu. "Recent Advances of Blockchain and Its Applications." *ACM Computing Surveys*, vol. 56, no. 1, 2023, pp. 1–39.
10. Khan, Muhammad Arif, Muhammad Tahir, and Imran Ashraf. "Blockchain-Based Secure Industrial IoT Framework for Smart Manufacturing." *Journal of Network and Computer Applications*, vol. 214, 2023, article 103618.
11. Sharma, Pradeep Kumar, and Neeraj Kumar. "Blockchain-Based Secure Communication in Internet of Things: Challenges and Opportunities." *IEEE Access*, vol. 11, 2023, pp. 43127–43146.
12. Singh, Rajesh Kumar, and Ruchi Mishra. "Blockchain Adoption in Smart Manufacturing Supply Chains: A Comprehensive Review." *Journal of Manufacturing Systems*, vol. 68, 2023, pp. 458–476.
13. Wang, Shuo, Yong Zhang, and Xiaofei Wang. "Blockchain and Edge Computing for Secure Industrial Internet of Things." *Future Generation Computer Systems*, vol. 142, 2023, pp. 373–386.
14. Yadav, Gunjan, and Sachin Kamble. "Digital Transformation of Automotive Supply Chains through Blockchain Technology." *Operations Management Research*, vol. 16, no. 3, 2023, pp. 812–828.
15. Zhang, Hui, and Wei Chen. "Blockchain-Based Product Traceability in Intelligent Manufacturing Systems." *Computers & Industrial Engineering*, vol. 176, 2023, article 108951.
16. Ahmed, Faizan, and Muhammad Usman. "Secure IoT Communication Framework Using Blockchain and Edge Intelligence." *IEEE Internet of Things Magazine*, vol. 7, no. 1, 2024, pp. 62–69.
17. Chen, Xiaolin, and Jun Wu. "Blockchain-Enabled Trust Management for Industrial Internet of Things." *IEEE Transactions on Industrial Informatics*, vol. 20, no. 2, 2024, pp. 1387–1398.
18. Gupta, Manish, and Rajeev Agrawal. "Enhancing Supply Chain Transparency through Blockchain and Smart Contracts." *International Journal of Production Economics*, vol. 268, 2024, article 109146.
19. Kumar, Anil, and Pawan Kumar. "Blockchain-Assisted Secure Logistics and Product Authentication in Smart Supply Chains." *Expert Systems with Applications*, vol. 243, 2024, article 122753.
20. Li, Yifan, and Ming Zhao. "Distributed Ledger Technologies for Automotive Manufacturing Ecosystems." *Journal of Industrial Information Integration*, vol. 39, 2024, article 100612.
21. Mishra, Biswaksen, Rajesh Kr. Singh, Ruchi Mishra, Denizhan Demirkol, and Tugrul Daim. "Blockchain Adoption in Automotive Supply Chain: A Systematic Literature Review Amalgamated with Bibliometric Analysis Technique and Future Research Directions." *Technology in Society*, vol. 81, 2025, article 102775.

22. Patel, Kevin. "AI+IoT+Blockchain Triad for Smart Traceability in the Automotive Industry." *International Journal of Research and Scientific Innovation*, vol. 12, no. 7, 2025, pp. 221–238.
23. García, José, and Mike Burmester. "Design of a Blockchain-Based Ubiquitous System for the Supply Chain with Autonomous Vehicles." *Electronics*, vol. 14, no. 23, 2025, article 4744.
24. Alharbi, Fahad, and Saeed Alotaibi. "Blockchain-Assisted Secure Communication Framework for Connected Vehicle Supply Chains." *IEEE Access*, vol. 13, 2025, pp. 18321–18340.
25. Rahman, Mohammad, and Ahmed Hassan. "Privacy-Preserving Blockchain Architecture for Industrial IoT Applications." *Future Internet*, vol. 17, no. 2, 2025, article 54.
26. Verma, Saurabh, and Deepak Gupta. "Smart Contracts for Transparent Manufacturing and Logistics Management." *Journal of Manufacturing Technology Management*, vol. 36, no. 1, 2025, pp. 88–109.
27. Zhao, Lin, and Kai Huang. "Scalable Permissioned Blockchain Framework for Industrial Supply Chain Networks." *IEEE Transactions on Engineering Management*, vol. 72, 2025, pp. 415–430.
28. Alghamdi, Abdullah, Nasim Ullah, and Ahmad Aziz Al-Ahmadi. "DeFiTrustChain: A DeFi-Enabled NFT and Escrow Framework for Secure Automotive Supply Chains in Smart Cities." *Sensors*, vol. 26, no. 1, 2026, article 315.
29. Kumar, Rakesh, and Priyanka Sharma. "Secure Blockchain-Enabled IoT Architecture for Industry 4.0 Supply Chain Applications." *Journal of Network and Systems Management*, vol. 34, no. 1, 2026, pp. 1–27.
30. Singh, Vivek, and Mohit Bansal. "Traceable and Transparent Automotive Supply Chains Using Blockchain, IoT, and Edge Computing." *International Journal of Information Management Data Insights*, vol. 6, no. 1, 2026, article 100312.