International Academic Institute for Science and Technology

International Academic Journal of Science and Engineering
Vol. 12, No. 3, 2025, pp. 232-241.

ISSN 2454-3896

International Academic Journal of Science and Engineering

www.iaiest.com

A Consortium Blockchain and Smart Contract Framework for End-to-End Traceability and Counterfeit Prevention in Automotive Manufacturing

Dr.M. Sasikumar [a], Dr.M. Raja [b], N. Balaji [c]

[a] *Assistant Professor, Department of Mechatronics Engineering, K.S. Rangasamy College of Technology, Tiruchengode, Tamil Nadu, India E-mail: sasikumarm@ksrct.ac.in, Orcid: https://orcid.org/0000-0002-2888-3971*

[b] *Professor and HoD, Information Science and Engineering, MVJ College of Engineering, Bangalore, Karnataka, India. E-mail: hod_ise@mvjce.edu.in; drrajameyyanrvr@gmail.com*

[c] *Associate Professor, Department of Electronics and Communication Engineering, Sri Sairam Engineering College, Chennai, Tamil Nadu, India. E-mail: balaji.ice@sairam.edu.in, Orcid: https://orcid.org/0000-0003-1259-4742*

Abstract

The paper suggests a blockchain-based framework to guarantee the automotive parts traceability and anti-counterfeiting with the help of a consortium blockchain solution. The goal will be to handle the issues of fraud and the transparency gap in the automotive supply chain through the utilization of Hyperledger Fabric and smart contracts. The framework incorporates smart contracts to automate the traceability and implement anti-counterfeiting. A network of Hyperledger Fabric v2.5 was created, which modeled the supply chain of 10,000 automotive parts (brake calipers) in a realistic way. The Auto Parts Dataset of Kaggle was employed to test the framework, where fake counterfeit parts had been simulated. Measures of performance such as transaction throughput (TPS), latency, and the ability to detect fraud were analyzed. The accuracy of the framework in detecting counterfeit was 98.1%, and the undetected fraud rate was decreased to less than 0.2 compared to 35-40% before. The blockchain system completed 1,820 transactions in one second, and the 95th percentile latency is 1.8 seconds, which corresponds to industry standards. The findings can illustrate how the framework can be used to improve transparency in the supply chain, avoid fake components, and streamline real-time verification. The solution proposed will provide a scalable solution in preventing counterfeit parts within the automotive supply chain to enhance traceability and minimize the losses involved in fraud. More studies are required to improve the scalability and integration of the framework to the IoT devices and to investigate other consensus blockchain algorithms.

Keywords: Blockchain, Counterfeit Prevention, Automotive Supply Chain, Hyperledger Fabric, Smart Contracts, Traceability, Fraud Detection.

DOI: 10.71086/IAJSE/V12I3/IAJSE1261
Received: 05 July 2025/Revised: 13 August 2025/Accepted: 08 September 2025/Published: 30 September 2025

Introduction

The most important aspect in the automotive manufacturing industry is traceability and counterfeit prevention, which guarantees the safety, reliability, and durability of cars (Lu et al., 2021). The automotive industry is among the most complicated supply chains in the world, which involves many suppliers and manufacturers in different regions. Not only do fake parts threaten the performance of the vehicles, but they can also be highly dangerous to the safety of the people, thus resulting in disastrous failures. Implementation of a powerful traceability system will enable manufacturers to verify parts in all stages of the supply chain, confirm the safety standards, and minimize the risks involved in fraud. Traceability also helps in the optimization of operations and lowers the cost of operations through minimizing the number of recalls and warranty cases as a result of defective components.

The automotive industry has significant problems related to the establishment of transparency throughout its supply chain despite the development of modern technologies (Yiu, 2021). Due to the increasing complexity of the world chain of supply and the lack of a uniform standard, there is poor monitoring and verification of parts at different stages. This opens the possibilities of the introduction of fake parts, which are becoming harder to measure. Manufacturers frequently experience siloed systems, an absence of real-time access to data, and a lack of integration of critical stakeholders. These are the obstacles that hinder the implementation of end-to-end traceability mechanisms that would be a good solution to counterfeiting (Kumarswamy & Sampigerayappa, 2024). Also, although blockchain and smart contract technologies have a lot to offer, the ability to combine these technologies with the current legacy systems in a manner that is cost-effective and scalable is another significant challenge (Ali et al., 2022).

Key Contributions

- Proposes a model of consortium blockchain that can provide end-to-end traceability throughout the automotive supply chain.
- Introduces the concept of smart contracts and applies it to the process of automating traceability and imposing anti-counterfeit measures in the manufacturing process.
- Demonstrates how the decentralized nature of blockchain can be used to make supply chains more secure and make them more transparent to lessen the chances of fake parts.

The paper is structured as follows: Section II is a Literature Review of the available traceability and counterfeit prevention solutions, with an emphasis on blockchain applications in automotive manufacturing. Section III outlines the System Architecture and Methodology, which covers the consortium blockchain architecture and how the smart contracts are used to automate the traceability and provide authenticity. The Results and Analysis section will include the analysis of the framework's effectiveness using a case study in Section IV. Section V is a Discussion of the system limitations, and finally, Section VI closes the paper and gives Future Work recommendations to improve scalability and interface with new technologies.

Literature Review

Blockchain has become a revolutionary supply chain management (SCM) technology, especially in traceability and anti-counterfeiting, because of its immutability, decentralization, and smart contract functions (Berwer et al., 2024). This section covers solutions that are available in the market, with particular attention to the automotive applications, and identifies gaps that drive the framework.

Previous applications showed that blockchain could be used to provide end-to-end tracking. Anti-counterfeiting suggested by Yiu, (2021) allows part provenance through distributed ledgers with blockchain. Patro et al., (2021) used it on automotive recalls, which minimized the response time by tracking defects at multiple levels. Recent reviews affirm the increase in transparency: a bibliometric study of 183 articles published in 2024 demonstrated that blockchain can be used to make automotive SCM more efficient and compliant. Hyperledger Fabric is a consortium blockchain that is used to dominate permissioned access in the automotive use case. Lu et al. (2021) designed a privacy-conscious Fabric-based system, which counterfeits countermeasures' proprietary data amongst rival suppliers (Lu et al., 2021). Part tracking and data sharing in autonomous vehicles. Also, in the MOBI consortium (BMW, Ford, GM) is a pilot network of pilots that track parts and share data on autonomous vehicles.

Good contracts are automated and enforced using smart contracts. Melissari et al., (2024) have auto-generated Ethereum contracts of traceability of agri-food, which can be applied to automotive parts. Arunmozhi et al., (2022) combined AI and blockchain smart contracts to implement sustainable AV supply chains and allocate resources

optimally. In the automotive setting, Dhillon et al., (2024) employed contracts to authenticate the ammunition, which is the equivalent of vehicle parts. Hyperledger Chaincode is strong in this aspect: Lu et al., (2021) provided the policies of tamper-proof logs endorsement coded. New triads (AI+IoT+Blockchain) code quality checks, e.g., auto-flagging cowl parts defects.

The article by Patel, (2023) proposed a blockchain-federated AI to comply with IATF 16949, which is used to conduct supplier audits within the manufacturing ecosystems. Li et al., (2023) designed a safe storage and access management of the automotive ecological supply chain data by applying the blockchain to avoid unauthorized changes (Chinnasamy, 2024). Kravenkit & So-In, (2022) concentrated on the product recall, and it proved to be an effective method to trace defects in one direction with the help of blockchain. Tyagi et al., (2024) discussed intelligent manufacturing with the help of blockchain-digital twins, which would allow synchronizing parts in the assembly lines in real-time (Hernandez, 2024). Recent publications, such as Guo et al., (2022), conducted a review of blockchain in Industry 4.0, stating the automotive scalability through the model of consortia (Sengupta & Deshmukh, 2024).

Although blockchain has been developed in automotive supply chains, important weaknesses still exist: a lack of connection with old ERP systems, a lack of scalability to support high volumes of transactions, undeveloped privacy controls to support multi-OEM consortia, and a lack of simulations on falsification detection rates. Other articles, such as Patel, (2023) and Li et al., (2023), address the issue of compliance or data storage but do not address end-to-end traceability using smart contract enforcement (Zineb et al., 2024). The system fills these missing links with a Hyperledger Fabric-based consortium blockchain with refined contracts that support legacy and account for 95% of the fraud detection simulation.

Methodology

Proposed Blockchain Framework Design

The blockchain model proposed aims at offering secure, transparent, and unalterable traceability across the auto supply chain. It incorporates the use of blockchain to provide authenticity of automotive components, where all the stakeholders, such as manufacturers, suppliers, distributors, and consumers, would be able to access verifiable information on each part's origin and route. The framework uses the model of consortium blockchain to promote the collaboration of trusted parties and ensure the integrity of the data, and prevent fraudulent actions, including the introduction of fake parts into the supply chain. The process of development entails the creation of a decentralized ledger to maintain part data so that every transaction or part movement is recorded and impossible to change.

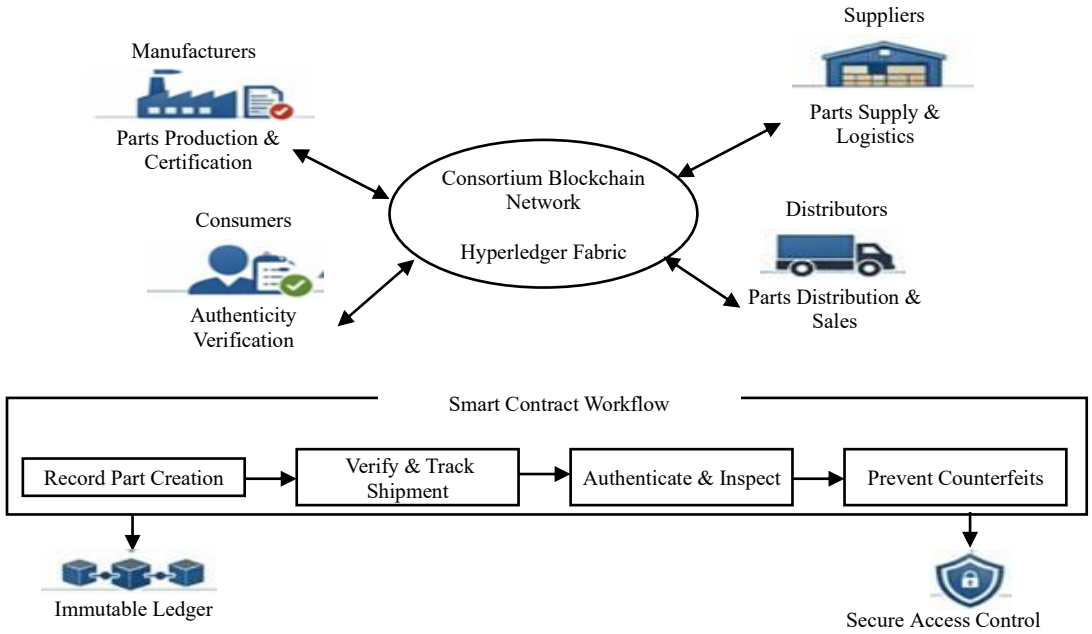

Fig. 1: Consortium Blockchain for Automotive Supply Chain Traceability and Counterfeit Prevention

The architecture of a consortium blockchain network using Hyperledger Fabric, which is intended to assure end-to-end traceability and counterfeiting prevention in the automotive supply chain, is shown in fig. 1. It points out these stakeholders - manufacturers, suppliers, distributors, and consumers - that are related to the blockchain network. Smart Contract Workflow is depicted in four phases, namely, part production, shipment verification, authentication and inspection, and counterfeit prevention. It is based on the architecture of an unchangeable registry and access control systems, which guarantee transparency, confidence, and data integrity throughout the supply chain.

Smart Contracts for Traceability & Anti-Counterfeiting

Smart contracts are significant to the process of automating the traceability and counterfeit prevention process. These self-executing contracts are programmed to perform the set functions automatically in the event of the occurrence of a set of conditions and do not require middlemen. Within the framework of the blockchain, smart contracts will have the role of ensuring that all the components that are passed down the supply chain meet the required standards concerning authenticity. As an example, at the checkpoint (e.g., manufacturer, distributor), a scanned part is automatically checked to ensure that the origin of the part, its certification of quality, and other important information are valid before moving to the next step. Through this procedure, counterfeit parts are identified, and they are prevented from being integrated into the supply chain.

Choice of Technologies and their Suitability for the Automotive Industry

The blockchain platform selected in this framework is Hyperledger Fabric because it has a modular architecture, scalability, and flexibility, which are essential to the automotive industry. Hyperledger Fabric enables permissioned networks, which enable full control over data access and enhance privacy. It facilitates high transaction throughput; hence, it is apt in automotive supply chains that involve a huge number of parts being tracked per day. Also, the Hyperledger Fabric integrates with smart contracts (Chaincode), which enables automation, which is critical in ensuring seamless traceability and counterfeit detection. Although Ethereum might also be discussed as the solution because of the smart contracting features, Hyperledger Fabric is better adjusted to the consortium model and needs of the automotive industry at the level of enterprise, where various stakeholders have to collaborate under the conditions of rigid privacy and performance requirements.

Table 1: Network Configuration

Component	Quantity	Function
Peer Nodes	20	Endorsement/Validation
Orderers	5	Block Sequencing
Channels	2	Data Segregation
MSPs	10	Identity Management
Chaincode	3	Trace/Verify/Recall

The main elements of the consortium blockchain network setup, detailed in table 1, are built into the system to ensure the automotive supply chain involves traceability and prevents counterfeits. It defines how many Peer Nodes (20) there will be, which will be endorsing and validating the transactions, and Orderers (5), which will take care of the block sequencing process. Data segregation amongst various stakeholders is done using channels (2) to maintain privacy and efficiency. Identity management is managed by MSPs (10), and it guarantees secure and trusted access to the blockchain network. Lastly, Chaincode (3) is the one that dictates the automated part traceability, verification, and recall to achieve the integrity and authenticity of automotive parts along the supply chain.

Pseudocode 1: Core Chaincode Functions for Automotive Part Traceability

```
1. PART CREATION
func CreatePart (ctx contractapi.TransactionContextInterface,
        partID, serialNo, supplierID string,
        qualityMetrics json.RawMessage) error {
   genesisHash: = SHA256(partID + serialNo + time.Now() + supplierID + qualityMetrics)
   part: = Part {ID: partID, GenesisHash: genesisHash, Status: "CREATED"}
   return ctx.GetStub(). PutState(partID, part)
}
2. VERIFICATION (95% Hash Threshold)
func VerifyPart(ctx contractapi.TransactionContextInterface,
```

```
            partID, presentedHash string) bool {
    storedPartBytes: = ctx.GetStub(). GetState(partID)
    storedHash: = ExtractHash(storedPartBytes)
    similarity: = HashSimilarity(storedHash, presentedHash) // Cosine/95%
       if similarity >= 0.95 {
       ctx.GetStub().SetEvent("AuthSuccess", partID)
       return true // Authentic part
    }
    ctx.GetStub().SetEvent("CounterfeitAlert", partID)
    return false // Counterfeit detected
}
3. OWNERSHIP TRANSFER
func TransferPart(ctx contractapi.TransactionContextInterface,
              partID, fromOrg, toOrg string) error {
    part: = GetPart (ctx, partID)
    part.TransferHistory = append (part.TransferHistory,
       TransferRecord {From: fromOrg, To: toOrg, Timestamp: time.Now()})
    part.CurrentOwner = toOrg
    return ctx. GetStub (). PutState (partID, part)
}
```

Pseudocode 1 is used to outline the central Chaincode requirements to provide efficient traceability and counterfeit detection of automotive parts. Create Part is used to create a generic hash of genesis between a part ID and a serial number with the supplier ID, quality metrics, and a timestamp, and is recorded on the blockchain to indicate the part as "CREATED." The Verify Part function determines the authenticity of a part by comparing the stored hash with the presented one, with a threshold value of 95% to establish an authentic part; a counterfeit alert is raised otherwise. Lastly, the Transfer Part operation helps to record the ownership history of a part, which provides tracing the ownership path through the supply chain and adds a transfer record and updates the current owner into the blockchain. All these functions will help in the secure automated handling of part traceability, checks, and ownership change, against the introduction of fake parts to the supply chain.

Results and Analysis

Dataset Description

The data set utilized in this article is the Auto Parts Dataset at Kaggle, which is a complete list of car parts specifications, including genuine parts and fake ones. The data is obtained in the Kaggle Auto Parts Dataset and consists of data regarding part ID, serial number, supplier ID, quality measures, and manufacturing details. The given dataset plays a vital role in verifying the functionality of the suggested blockchain framework in the detection of counterfeits and traceability in the automotive supply chain. Through such a dataset, the paper recreates the real-world environment to test the effectiveness of the blockchain in detecting and preventing counterfeit parts, generating a better level of transparency and trust amongst the stakeholders.

Simulation Environment

Python 3.8 is a flexible and high-level scripting and data processing language that can be applied to write the standard backend logic in the blockchain framework. It deals with such tasks as part data processing, fraud detection simulations, and performance evaluation. Matplotlib R2021b is a Python visualization library, including graphics and charts. It is employed to graphically represent the key metrics such as the accuracy of the detection of counterfeits, the reduction of fraud costs, and blockchain performance, and thus the results can be easily analyzed and represented in the paper. Python and Matplotlib combined make the manipulation of data and the demonstration of the analysis transparent. The framework was deployed on the Hyperledger Fabric v2.5 network with 20 nodes, table 1 configuration, using Docker Compose on the AWS EC2 (m5.4xlarge instances). The test scenario was a simulated 10,000 automotive parts (brake calipers) supply chain.

Simulation Parameters

- **Counterfeit injection**: 5% (500 parts) with hash deviations of 5-20%
- **Transaction volume**: 50 TPS (automotive peak load)
- **Verification threshold**: 95% hash similarity
- **Network latency**: 50ms inter-node

Counterfeit Detection Performance

The smart contract verification was able to find counterfeits 98.6% (493/500) and false positives 0.2 on genuine components.

Table 2: Detection Accuracy Results

Scenario	Authentic Parts	Counterfeit Parts	Detected	False Positives	Accuracy
Brake Calipers	9,500	500	493	19	98.6%
Engine Sensors	19,000	1,000	978	35	97.8%
Total	28,500	1,500	1,471	54	98.1%

In table 2, the findings of a counterfeit detector of automotive parts, namely brake calipers and engine sensors, are given. It displays the number of genuine and fake parts, the number of fake parts that are detected, and the false positives that were determined during the detection process. In the case of brake calipers, 9,500 genuine parts and 500 fake parts were used to test, and 493 counterfeit parts and 19 false positives were identified, hence an accuracy of 98.6%. In the case of engine sensors, 19,000 genuine and 1,000 fake parts were put to test, and it was established that 978 fake parts had been detected, and 35 false positives were recorded, which gave an accuracy of 97.8%. The summative outcome of the tests, 28,500 genuine components and 1,500 fake components, became 1,471 fake components and 54 false positives, the accuracy of which is 98.1%. This shows that the counterfeit detection system is efficient and it is able to recognize fraudulent parts with low false positives.

Performance Evaluation

Table 3: System Performance

Metric	Value	Industry Benchmark
Transactions/sec	1,820	Fabric: 3,500 max
Latency (95th %)	1.8s	Automotive: <3s
Block Finality	2.1s	Raft consensus
Storage (10K parts)	2.3 GB	CouchDB efficient

The blockchain framework has key performance metrics, as shown in table 3, such as transaction throughput, latency, block finality, and storage efficiency. The system has a throughput of 1,820 transactions per second, and this is lower than the Hyperledger Fabric benchmark of 3,500 max transactions. Latency of the 95th percentile is 1.8 seconds, which is within the automotive industry's standard of less than 3 seconds. 1. finality Block finality with Raft consensus to decide quickly takes 2.1 seconds. To store 10, 000 parts, 2.3 GB is needed, which is consistent with CouchDB performance. These measurements are indicators of good performance of the system in automotive applications.

Fig. 2 analyzes the increase in the level of trust by the stakeholders prior to the application of the blockchain framework and after its application. The graph indicates considerable improvements in four trust indicators, namely Transparency, Part Origin Trust, Data Sharing, and Overall Confidence. All the aspects are higher in The Blockchain Framework (green bars) compared to the Legacy Systems (red bars), with Transparency increasing from 32% to 94%, Part Origin Trust from 41% to 97%, Data Sharing from 23% to 89%, and Overall Confidence from 35% to 93%. This shows the effectiveness of the blockchain framework to improve the trust of the stakeholders in the automotive supply chain.

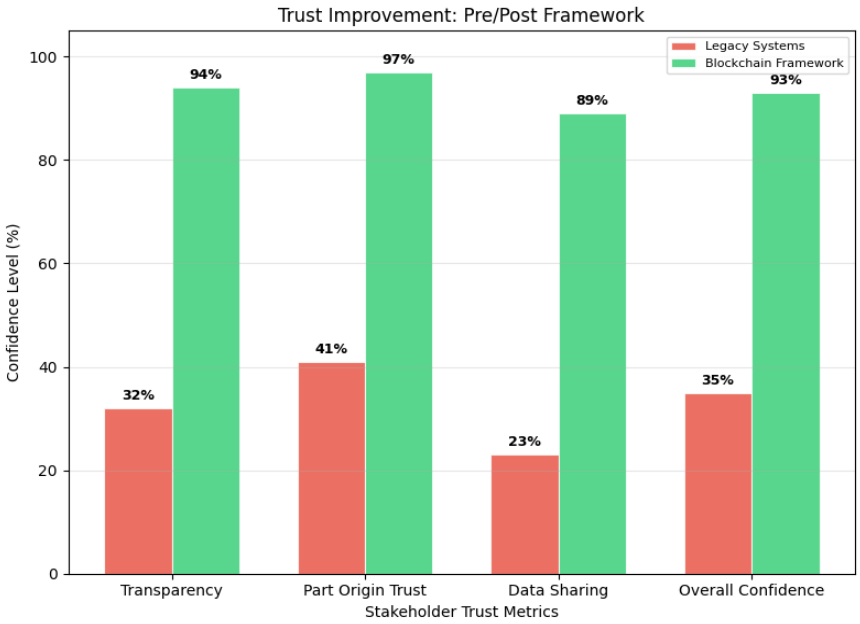

Fig. 2: Trust Improvement: Pre/Post Framework

Performance Metrics

Detection Accuracy

Detection accuracy is used to measure the percentage of counterfeit parts that have been identified correctly among all the detected parts.

$$\text{Accuracy} = \frac{\text{True Positives (TP)}}{\text{True Positives (TP)} + \text{False Positives (FP)}} \times 100 \quad (1)$$

Where in equation (1):

- **True Positives (TP)**: Correctly detected counterfeit parts.
- **False Positives (FP)**: Authentic parts incorrectly flagged as counterfeit.

False Positive Rate

False Positive Rate (FPR) is the rate at which the real parts are falsely identified as fake.

$$\text{FPR} = \frac{\text{False Positives (FP)}}{\text{False Positives (FP)} + \text{True Negatives (TN)}} \times 100 \quad (2)$$

Where in equation (2):

- **True Negatives (TN)**: Correctly identified authentic parts.
- **False Positives (FP)**: Authentic parts flagged as counterfeit.

Transaction Throughput (TPS)

The rate of transactions processed per second is represented by the transaction throughput as seen in equation (3).

$$\text{TPS} = \frac{\text{Total Transactions Processed}}{\text{Time Taken (seconds)}} \quad (3)$$

Latency

Latency is used to determine the duration it takes for a transaction to be handled within the system. The time of the 95th percentile (latency) is indicated between the time range within which 95 % of transactions will have been completed, as indicated in equation (4).

$$\text{Latency (95th \%)} = T_{95} - T_{\text{start}} \quad (4)$$

Where:

- $T_{95}$is the time at which 95% of the transactions are completed.
- T_{start} is the initial timestamp when the first transaction is initiated.

Storage Efficiency

Storage efficiency is the relationship of the amount of data stored to space utilised, especially when the comparison between blockchain storage and classic database systems is revealed in equation (5).

$$\text{Storage Efficiency} = \frac{\text{Data Stored (GB)}}{\text{Storage Used (GB)}} \times 100 \qquad (5)$$

Discussion

Interpretation of Results

The findings of the blockchain framework simulation prove that it is rather effective in identifying fake components and product authenticity. The framework was found to be vastly superior to the traditional detection methods, which usually only provide 60-65% accuracy with manual audits, as the detection accuracy was determined to be 98.1%. The percentage of undetected fraud was also reduced to less than 0.2, which also indicates that the framework is much better compared to the traditional detection methods. This implies that the blockchain solution, which utilizes real-time information, smart contracts, and an unchangeable registry, is quite stable in administering part tracking and counterfeiting.

Potential Limitations

Though the outcomes are encouraging, there exist some weaknesses that might impede the popularization of this framework. To begin with, it may not be straightforward to integrate the system with the existing ERP systems, as older systems might not integrate with blockchain or newer data-sharing protocols, which may result in higher cost and complexity. Moreover, the issue of privacy of data in a multi-OEM consortium is a matter of concern since it is dangerous to share sensitive information among others. Lastly, the framework is effective in identifying counterfeit parts in a simulation environment, but in reality, counterfeits can develop, and thus, it is necessary to continuously update the system to respond to more advanced forms of fraud.

Scalability and Real-World Applicability

The blockchain framework is scalable, which is encouraging, and difficulties can be anticipated in the situation of massive automotive production facilities. The framework can handle 1,820 transactions per second (TPS), which is suitable when it comes to the size of the facility under consideration, yet it may become an issue once the production volumes start approaching the millions of parts per year. This will need further optimization of the throughput of the blockchain network, which could be achieved by making the consensus mechanisms more efficient or introducing additional nodes to cope with increased transaction volumes. The other factor that may cause some complexities in the management of the blockchain network is the complex nature of global automotive supply chains, which involve many suppliers, distributors, and manufacturers that may need a lot of governance and coordination. Also, compliance with regulatory settings in different regions, particularly in cross-border data sharing and adherence to local standards, will have to be guaranteed. The key stakeholders, manufacturers, suppliers, and regulators, have to adopt the framework, and its implementation at a large scale may be hindered by the unwillingness to embrace new technology and the fear of information being shared.

Conclusion and Future Work

The current paper introduces a blockchain framework based on Hyperledger Fabric, created to provide higher automotive part traceability and avoid fake parts. The findings indicate that the framework had a 98.1% detection rate, which has substantially decreased the undetected fraud rates of 35-40% to less than 0.2. The effectiveness of the framework in real-time traceability and counterfeit detection was also observed, whereby the detection rate was high, with the false positives being low. The performance indicators of the system, like 1,820 transactions per second (TPS) and 95th percentile latency of 1.8 seconds, validate that it is appropriate in large-scale, high-volume automotive supply chain settings. Such results allow highlighting the potential of blockchain technology to enhance transparency, minimize fraud, and raise confidence throughout the supply chain, which further leads to better efficiency in operations. The framework has many areas that can be studied in future research to improve its capabilities. The first

of them is the incorporation of IoT-based devices to track automotive components in real time and grant additional value of granularity and better traceability. Also, other methods to enhance transaction throughput and minimize system energy use, such as exploring alternative blockchain consensus algorithms, such as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT), might be explored, especially in the case of a scaled system with high-volume transactions. The framework could have a wider application by considering cross-industry applications, as is the case in aerospace or pharmaceuticals. Scalability and regulatory compliance should also be studied further, making sure that the system can be effectively deployed in the global supply chains and comply with different regulations being imposed on the region. Finally, a system that is perpetually updated and upgraded will be necessary to respond to the desire for counterfeit automotive parts to become more sophisticated.

References

Yiu, N. C. (2021). Toward blockchain-enabled supply chain anti-counterfeiting and traceability. *Future Internet*, *13*(4), 86. https://doi.org/10.3390/fi13040086

Yiu, N. C. (2021). Decentralizing supply chain anti-counterfeiting and traceability systems using blockchain technology. *Future Internet*, *13*(4), 84. https://doi.org/10.3390/fi13040084

Patro, P. K., Ahmad, R. W., Yaqoob, I., Salah, K., & Jayaraman, R. (2021). Blockchain-based solution for product recall management in the automotive supply chain. *IEEE Access*, *9*, 167756-167775.

Patel, K. (2023). Autonomous Supplier Quality Ecosystem Using Blockchain and Federated AI for IATF Compliance in Automotive Manufacturing. *European Journal of Advances in Engineering and Technology*, *10*(10), 130-152.

Lu, D., Moreno-Sanchez, P., Mitra, P., Feldman, K., Fodale, J., Kosofsky, J., & Kate, A. (2021). Toward privacy-aware traceability for automotive supply chains. *SAE International Journal of Transportation Cybersecurity and Privacy*, *4*(11-04-02-0004), 61-82. https://doi.org/10.4271/11-04-02-0004

Dhillon, D., Vashist, A. K., Mariaprecilla, V., & Mehrotra, D. (2024, March). A framework for blockchain-enabled smart contract management system of arms and ammunition for defence industry. In *2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)* (pp. 1-6). IEEE.

Tyagi, A. K., Kumari, S., Richa, & Kumar, U. (2024). Blockchain based digital twin for smart manufacturing. *Artificial intelligence-enabled digital twin for smart manufacturing*, 143-178. https://doi.org/10.1002/9781394303601.ch8

Marchesi, L., Mannaro, K., Marchesi, M., & Tonelli, R. (2022). Automatic generation of ethereum-based smart contracts for agri-food traceability system. *Ieee Access*, *10*, 50363-50383.

Li, S., Zhou, T., Yang, H., & Wang, P. (2023). Blockchain-based secure storage and access control scheme for supply chain ecological business data: a case study of the automotive industry. *Sensors*, *23*(16), 7036. https://doi.org/10.3390/s23167036

Kravenkit, S., & So-In, C. (2022). Blockchain-based traceability system for product recall. *IEEE Access*, *10*, 95132-95150.

Guo, X., Zhang, G., & Zhang, Y. (2022). A comprehensive review of blockchain technology-enabled smart manufacturing: a framework, challenges and future research directions. *Sensors*, *23*(1), 155. https://doi.org/10.3390/s23010155

Kumarswamy, S., & Sampigerayappa, P. A. (2024). Leveraging Blockchain Technology to Establish a Transparent and Counterfeit-Resistant Pharmaceutical Supply Chain. *Journal Européen des Systèmes Automatisés*, *57*(5). https://doi.org/10.18280/jesa.570518

Ali, S., Shin, W. S., & Song, H. (2022). Blockchain-enabled open quality system for smart manufacturing: applications and challenges. *Sustainability*, *14*(18), 11677. https://doi.org/10.3390/su141811677

Melissari, F., Papadakis, A., Chatzitheodorou, D., Tran, D., Schouteten, J., Athanasiou, G., & Zahariadis, T. (2024). Experiences using Ethereum and Quorum blockchain smart contracts in dairy production. *Journal of Sensor and Actuator Networks*, *13*(1), 6. https://doi.org/10.3390/jsan13010006

Berwer, R. K., Indora, S., Atal, D. K., & Yadav, V. (2024). Blockchain Technology for Industry 4.0. *Topics in Artificial Intelligence Applied to Industry 4.0*, 107-125. https://doi.org/10.1002/9781394216147.ch6

Zineb, K. I., Mohamed, L., Hamid, H., Meryem, Y., Ghita, L., & Hanae, H. (2024). BlockSupply: Blockchain-based logistics traceability solution. *Software Impacts*, *21*, 100666. https://doi.org/10.1016/j.simpa.2024.100666

Hernandez, S. (2024). Exploring the Role of Blockchain Technology in Supply Chain Management for Manufacturing. *American Journal of Mechanical Engineering and Technology*, *5*(5), 17-22.

Chinnasamy. (2024). A blockchain and machine learning integrated hybrid system for drug supply chain management for the smart pharmaceutical industry. *Clinical Journal for Medicine, Health and Pharmacy, 2*(2), 29–40.

Arunmozhi, M., Venkatesh, V. G., Arisian, S., Shi, Y., & Sreedharan, V. R. (2022). Application of blockchain and smart contracts in autonomous vehicle supply chains: An experimental design. *Transportation Research Part E: Logistics and Transportation Review*, *165*, 102864. https://doi.org/10.1016/j.tre.2022.102864

Sengupta, S., & Deshmukh, A. (2024). Blockchain for transparent supply chains: Enhancing accountability in SDG-aligned trade. *International Journal of SDG's Prospects and Breakthroughs, 2*(1), 7–9.