A Blockchain-Enabled Framework for Secure Vehicle Lifecycle Management

Sayali Parab[1], Chayan Bhattacharjee[2]

[1]Lecturer, Department of Information Technology, SES's L. S. Raheja College of Arts & Commerce, Mumbai, India
[2]Lecturer, Department of Information Technology, Chikitsak Samuha's Patkar Varde College, Mumbai, India

Abstract
The automotive sector suffers from fragmented records for vehicle ownership, servicing, insurance, and regulatory compliance. These silos permit frauds such as odometer manipulation, fake service histories, duplicate registration documents, and fraudulent insurance claims, reducing trust in secondary markets and complicating regulatory enforcement. This paper proposes a permissioned blockchain-based Vehicle Lifecycle Management (VLM) model that records manufacturing, registration, servicing, ownership transfers, accident reports, and insurance events as immutable transactions. The model leverages cryptographic hashing, decentralized peers (manufacturers, service centers, insurers, RTOs), permissioned consensus (e.g., PBFT/RAFT), smart contracts for automated transfers and claims, and encryption for privacy. Primary case studies (BMW Part Chain, Hyundai MOBIUS, Renault initiatives, IBM Hyperledger pilots) are analyzed to validate feasibility. Evaluation metrics include fraud reduction potential, verification time improvement, interoperability, and privacy. The paper concludes with findings on benefits, implementation challenges, and recommended next steps for pilot deployment.

Keywords: Blockchain, Vehicle Lifecycle, Ownership Tracking, Service Records, Smart Contracts, Permissioned Ledger, Automotive Fraud

1. Introduction

Vehicles progress through stages: manufacturing, registration, service, ownership transfer, accident/insurance events, and resale. Each stage is managed by distinct stakeholders using disparate systems. The absence of a single, verifiable, tamper-resistant record undermines buyer trust, increases fraud, and complicates regulatory oversight.

Current centralized or siloed information management enables odometer tampering and falsified service records, counterfeit or duplicate registration/insurance documents, delayed or fraudulent insurance claims, difficult and slow cross-stakeholder verification (manufacturers, workshops, insurers, RTOs).

The objective is to design and evaluate a blockchain-based Vehicle Lifecycle Management (VLM) model that preserves immutable service and ownership history, automates ownership transfer and claims processes via smart contracts, balances transparency and privacy and is pragmatic for industry and regulatory adoption.

The scope of the research is to focus on the architecture, components, and practical considerations of a permissioned blockchain VLM in automotive ecosystems. It excludes low-level consensus protocol proofs and full economic incentive modeling

2. Literature Review

A. World Economic Forum, Blockchain for Supply Chains, 2020 and Hyperledger Foundation, Enterprise Blockchain Case Studies, 2022.

Blockchain has been extensively studied as a technology for improving transparency, traceability, and trust in supply chain systems. Its inherent properties—immutability, distributed consensus, and secure record keeping—make it well suited for tracking asset provenance and lifecycle events (World Economic Forum, 2020). In mobility and automotive domains, blockchain-based solutions have been explored for recording vehicle histories, parts provenance, and maintenance data. Industry pilots by manufacturers such as BMW, Renault, and Hyundai demonstrate the practical feasibility of using blockchain to securely log service records and component origins (Hyperledger Foundation, 2022). While these initiatives validate the technology's potential, most remain limited to pilot-scale deployments.

B. Ethereum Foundation, Introduction to Smart Contracts, 2021

Smart contracts enable automated execution of transactions based on predefined conditions, reducing the need for manual intervention and intermediaries. Prior work highlights their effectiveness in automating ownership transfers, compliance checks, and payment settlements, thereby reducing transaction time and administrative overhead (Ethereum Foundation, 2021). In supply chain and mobility applications, smart contracts support rule-based enforcement of workflows and improve data consistency across stakeholders. However, existing studies largely focus on conceptual or isolated use cases, with limited emphasis on integration into regulatory and institutional processes.

C. E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," Proc. EuroSys, 2018.

Enterprise and regulated environments often require controlled participation, data privacy, and identity management. Permissioned blockchain platforms, such as Hyperledger Fabric, address these requirements by supporting authenticated membership, role-based access control, and modular consensus mechanisms (Androulaki et al., 2018). Such platforms are well suited for multi-stakeholder ecosystems involving manufacturers, service centers, insurers, and regulatory bodies. Despite their architectural advantages, prior literature offers limited discussion on real-world adoption challenges and interoperability across diverse organizational actors.

Research Gap

Although prior research and industry pilots demonstrate the applicability of blockchain in supply chains and mobility, a clear integration gap exists. Current literature lacks standardized frameworks that combine regulatory workflows, insurance claim automation, and workshop-level participation within a unified blockchain system. This paper addresses this gap by proposing an integrated, permissioned blockchain framework that aligns smart contract automation with regulatory and operational requirements across the mobility ecosystem.

3. Research Methodology

This study follows a descriptive–analytical research design combining qualitative case-study analysis and system modeling. Industry blockchain pilots by BMW, Hyundai, Renault, and IBM are examined to

identify practical design patterns and implementation constraints. Based on these insights, a permissioned blockchain–based Vehicle Lifecycle Management (VLM) architecture is conceptually designed.
Data for the study is obtained from publicly available project reports and whitepapers (e.g., BMW PartChain, Hyundai MOBIUS, IBM Hyperledger pilots), industry standards and analyses published by organizations such as the Hyperledger Foundation and the World Economic Forum, and peer-reviewed academic literature on blockchain adoption in regulated domains.
The proposed VLM model defines key architectural elements, including data flows, transaction types, smart contract templates, and access-control mechanisms within a permissioned blockchain environment. The framework is evaluated qualitatively using criteria such as fraud reduction potential, verification latency, privacy preservation, and interoperability among ecosystem participants.
The methodology assumes active participation from manufacturers and regulatory authorities, such as Regional Transport Offices (RTOs), and the feasibility of maintaining digitized legal records within existing regulatory frameworks. Policy variability and institutional readiness are recognized as practical constraints.

4. Proposed System Design

The proposed Vehicle Lifecycle Management (VLM) system is implemented as a permissioned blockchain network in which authorized participants—including manufacturers, Regional Transport Offices (RTOs), insurers, certified service centers, and dealers—validate and record vehicle-related events. Each participant operates a permissioned node with role-specific access rights.
At vehicle production, the manufacturer initializes a unique Vehicle Identity (VID) and records factory-fitted components and recall information. Certified service centers append service and repair records, including part replacements. Insurance nodes manage policy issuance, renewals, and claims, with smart contracts supporting automated claim evaluation. RTO nodes verify digital registration records, approve ownership transfers, and enforce regulatory constraints, while vehicle owners or buyers access permitted data and initiate transfer requests using cryptographic keys.
The system supports multiple transaction types, including VID creation, service events, ownership transfer via smart contracts, insurance claim processing, and regulatory document updates. To preserve privacy, sensitive data is stored off-chain, with cryptographic hashes and access pointers recorded on-chain. Access control is enforced using asymmetric encryption and attribute-based permissions.
A permissioned consensus mechanism such as PBFT or RAFT is employed to achieve low-latency finality and high throughput among trusted participants. For high-frequency data, such as telematics, state channels or sidechains are used to improve scalability.

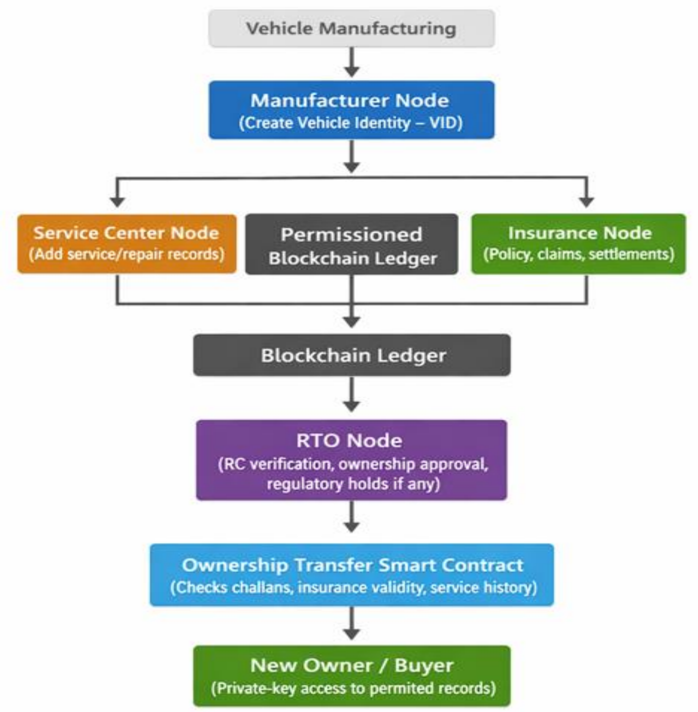

Fig 1. Proposed System Design

5. Mapping Blockchain Components to the Vehicle Lifecycle

Each stage of the vehicle lifecycle is represented on the blockchain through well-defined digital mechanisms that ensure data integrity, transparency, and controlled access.

A. Transaction Representation

Every significant lifecycle event is recorded as a cryptographically signed transaction. For instance, a service event transaction captures structured service details along with a hash of the corresponding invoice, creating a permanent and verifiable service record. This approach ensures that operational data, once recorded, cannot be altered or repudiated.

B. Immutable Ledger

The distributed ledger maintains a complete and chronological history of vehicle-related events. Its immutability prevents retroactive modification of records, making it particularly effective in mitigating fraudulent practices such as odometer tampering, falsified service histories, and unauthorized record alterations.

C. Decentralized Validation

Transaction validation is distributed across multiple authorized peers within the network, including manufacturers, service providers, insurers, and regulators. This decentralized design removes reliance on a single controlling authority and ensures that no individual stakeholder can unilaterally manipulate or suppress records.

D. Cryptographic Security

Public-key cryptography is employed to establish and verify ownership credentials, while a combination of symmetric and asymmetric encryption techniques is used to protect sensitive off-chain data. This layered security model ensures confidentiality without compromising the verifiability of on-chain records.

E. Consensus Mechanism

To achieve timely confirmation and operational efficiency, permissioned consensus protocols such as

Practical Byzantine Fault Tolerance (PBFT) or RAFT are utilized. These mechanisms provide fast transaction finality and reliability, making them suitable for enterprise-grade and regulated environments.

F. Smart Contract Automation

Smart contract templates encode business logic across the vehicle lifecycle. These include automated ownership transfer checks that verify pending regulatory dues and insurance validity, conditional release of insurance claim funds upon validated damage assessments, and warranty verification linked to authentic part identifiers recorded at the manufacturing stage.

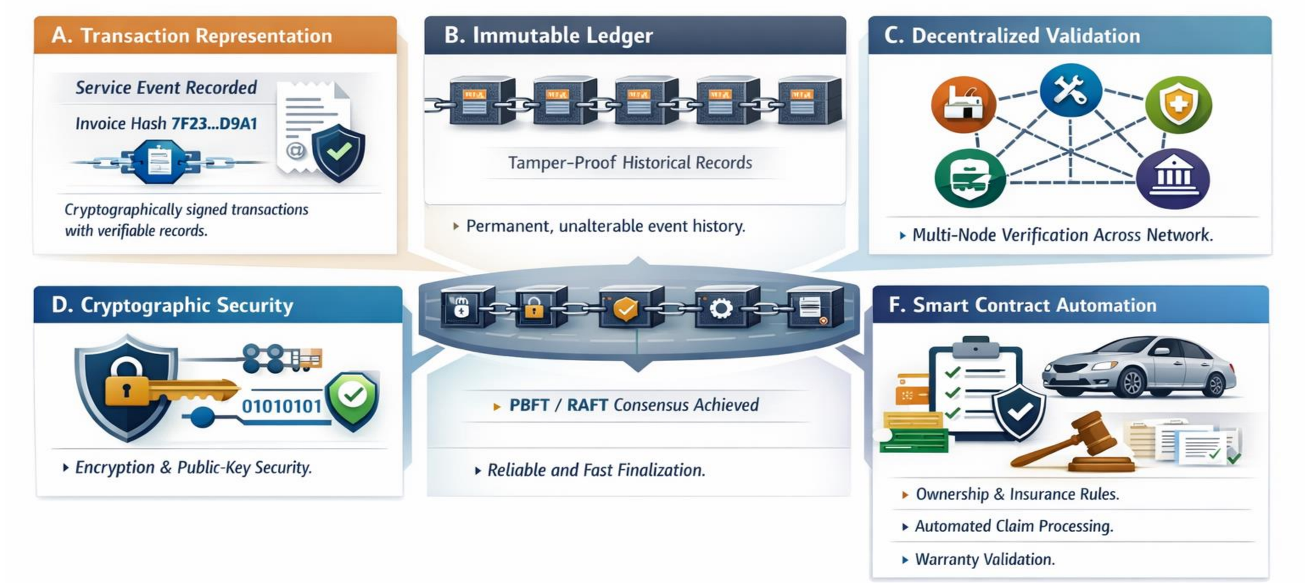

Fig 2. Mapping Blockchain Components to the Vehicle Lifecycle

6. Benefits, Risks, and Mitigation

A. Benefits

The proposed blockchain-based Vehicle Lifecycle Management system offers a decentralized and trustworthy source of vehicle history, enabling consistent and verifiable records across the ecosystem. Automation through smart contracts can significantly accelerate regulatory and insurance-related processes, reducing administrative delays and manual verification. Enhanced transparency improves buyer confidence, particularly in the secondary vehicle market, where access to authentic service and ownership histories is critical. Additionally, immutable records help curb fraudulent insurance claims and limit the circulation of counterfeit or uncertified vehicle parts.

B. Risks

Despite its advantages, the system faces several practical and institutional risks. Regulatory acceptance and legal recognition of blockchain-maintained records remain uncertain and may vary across jurisdictions. Data privacy concerns, particularly relating to the handling of ownership-related personally identifiable information, must be carefully addressed to comply with data protection regulations. The cost and operational complexity of establishing and governing a multi-stakeholder blockchain network also pose challenges, as does potential resistance from organizations reliant on legacy systems and processes.

C. Mitigation Strategies

To address regulatory risks, close collaboration with government authorities is essential to ensure formal acceptance of blockchain-backed registration certificates and digitally signed records. Privacy risks can be mitigated by storing sensitive personal data off-chain and recording only cryptographic hashes on the blockchain. Governance and operational complexity are reduced through the use of permissioned networks that clearly define roles, access rights, and responsibilities. Finally, phased deployment strategies—such as piloting the system within a single state or with a limited set of manufacturers—can facilitate gradual adoption and risk-controlled scaling.

References

1. E. Androulaki et al., "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in Proceedings of the 13th EuroSys Conference, 2018. DOI: https://doi.org/10.1145/3190508.3190538
2. K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016. DOI: https://doi.org/10.1109/ACCESS.2016.2566339
3. M. Kouhizadeh and J. Sarkis, "Blockchain practices, potentials, and perspectives in sustainable supply chains," Computers & Industrial Engineering, vol. 138, pp. 106–115, 2018. DOI: https://doi.org/10.1016/j.cie.2018.12.030
4. T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the application of blockchain to Industry 4.0 smart factories," IEEE Access, vol. 7, pp. 45201–45218, 2019. DOI: https://doi.org/10.1109/ACCESS.2019.2908780
5. X. Xu, I. Weber, and M. Staples, Architecture for Blockchain Applications. Cham, Switzerland: Springer, 2019. DOI: https://doi.org/10.1007/978-3-030-03035-4
6. N. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," Procedia Computer Science, vol. 132, pp. 1815–1823, 2018. DOI: https://doi.org/10.1016/j.procs.2018.05.143
7. S. Mou, Q. Xu, and J. Yang, "Research on blockchain-based insurance business models," Journal of Physics: Conference Series, vol. 1453, no. 1, p. 012103, 2020. DOI: https://doi.org/10.1088/1742-6596/1453/1/012103
8. Z. Yang, Z. Xiong, X. Zhao, D. Niyato, and J. Zhang, "Deep learning-based IoT security: A review and case studies," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7828–7839, 2019. DOI: https://doi.org/10.1109/JIOT.2019.2918285