Blockchain Technology for the Automotive Sector

Abstract

The automotive sector is one of the most data-intensive industrial ecosystems in the global economy, and its value chain depends on information that crosses organizational, jurisdictional, and lifecycle boundaries. The current data infrastructure, organized around isolated proprietary databases under unilateral stakeholder control, leaves multiple persistent trust gaps along the vehicle lifecycle. Among them, this thesis addresses four: opacity in automotive supply-chain sustainability, absence of verifiable digital product passports for regulated vehicle components, information asymmetries in second-hand vehicle markets, and untransparent municipal governance of road infrastructure. The four gaps share a single structural cause: the absence of a decentralized, tamper-evident, and auditable data infrastructure.

This thesis investigates blockchain as a unifying trust infrastructure for the automotive ecosystem and develops four engineering contributions that address the gaps in lifecycle order. The first contribution combines blockchain with fully homomorphic encryption on Zama's fhEVM to enable supplier sustainability indices to be computed on encrypted KPIs without raw data disclosure. The second contribution is a provision-by-provision analysis demonstrating that blockchain jointly satisfies the technical requirements imposed by EU Regulation 2023/1542 on digital battery passports, covering decentralized storage, data authentication, differentiated access control, and ownership-linked data responsibility. The third contribution is a dynamic, role-gated, lockable ERC-721 vehicle NFT with per-field state-machine governance and an integrated decentralized marketplace, supporting multi-stakeholder updates from OEMs, insurers, inspectors, and repair shops. The fourth contribution is a three-contract coordination layer for municipal pothole management, combining ERC-2771 meta-transactions for gasless multi-source reporting, an ERC-20 incentive minted on validation, grid-based spatial duplicate detection, and a multi-factor priority-scoring algorithm.

Beyond the individual contributions, a cross-cutting analysis recovers three architectural patterns that recur across the four systems: hybrid on-chain/off-chain storage with content-addressed bridging, role-based access control with policy-driven asymmetry inversion, and state machines for lifecycle-bound mutable state. The analysis then positions the contributions on a single privacy–transparency spectrum spanning from encrypted-by-default computation on private data, through differentiated regulatory access, to fully public verifiability. The same architectural primitives serve opposite policy goals on this spectrum depending on whether the application protects confidentiality or provenance. Normalized cost analysis, Slither-based security assessment, and direct comparison with federated-data-space alternatives such as Catena-X situate the work within the broader landscape of European industrial digital infrastructure.

The thesis concludes that blockchain, in the architectural configurations developed here, is technically capable and economically viable for the four classes of automotive trust gap, under bounding conditions stated explicitly: trust in institutional anchors at the attestation layer, the maturity of the fhEVM infrastructure for the encrypted-computation regime, and the gap between prototype and production deployment. The architectural vocabulary recovered from the four contributions is positioned as a foundation for the broader project of building verifiable digital infrastructures for the European automotive sector.