Blockchain Trilemma in Autonomous Intelligent Vehicles: Technical Approaches for Security, Speed, and Scalability

Amadi Chimeremma Sandra, Taesoo Jun

Department of IT Convergence Engineering,Kumoh National Institute of Technology, Gumi, South Korea

Abstract

Autonomous Intelligent Vehicles (AIVs) require secure, low-latency, and scalable communication frameworks to support safety critical decision-making in dynamic traffic environments. Blockchain deployment in AIVs is constrained by the blockchain trilemma the difficulty of simultaneously optimizing security, speed, and scalability. This paper reframes the trilemma for vehicular contexts and introduces innovation driven solutions, including hybrid consensus mechanisms, edge-enabled blockchain layers, AI-augmented security modules, and lightweight cryptography. Case studies of urban intersections and highway platooning demonstrate that tiered blockchain architectures, combined with AI-driven anomaly detection and validator selection, can achieve consensus latencies under 200 ms while ensuring authenticated logging and scalable coordination across hundreds of vehicles. Finally, open challenges such as hardware resource limits, energy overhead, interoperability with legacy infrastructure, and quantum-era threats are discussed, alongside future directions in adaptive consensus, quantum-safe cryptography, and 6G-integrated vehicular networks.

Keywords: Autonomous Intelligent Vehicles, Blockchain Trilemma, Hybrid Consensus, Edge Blockchain, AI Security, Scalability, Vehicular Networks.

1. Introduction

Autonomous Intelligent Vehicles (AIVs) rely on real-time, secure communication across Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) channels, where milliseconds of delay or data tampering can compromise safety. Blockchain offers a decentralized and tamper-resistant framework for authenticated, immutable data exchange in such environments [1]. However, the blockchain trilemma balancing security, speed, and scalability remains a major barrier [2]. Traditional systems like Bitcoin prioritize security at the cost of throughput, while sharding and off-chain channels improve scalability but weaken trust [3]. To meet AIV demands for sub-200 ms consensus and scalable coordination, this study:

- Reframes the blockchain trilemma for AIVs, analyzing trade-offs among security, speed, and scalability.
- Proposes innovation-driven strategies to mitigate these constraints.
- Validates the approach through case studies on secure, low-latency vehicular coordination.

Figure 1 illustrates the delicate balance between security, speed, and scalability in AIV ecosystems

Figure 1: Blockchain trilemma in Autonomous Intelligent Vehicles (AIVs), highlighting the trade-offs among security, speed, and scalability

2. Innovation Driven Strategies for Blockchain AIVs

The blockchain trilemma in Autonomous Intelligent Vehicles (AIVs) requires rethinking architectures to balance security, speed, and scalability under real-time constraints. Conventional approaches such as Proof-of-Work and centralized storage are limited by latency, energy use, and single points of failure. To address these gaps, four innovation driven strategies; hybrid consensus, edge–blockchain integration, AI-augmented security, and lightweight cryptography have been proposed. Hybrid consensus combines low-latency PBFT with scalable PoS or PoA synchronization to ensure sub-200 ms safety-critical decisions [4]. Edge computing shifts blockchain processing to roadside units, reducing propagation delay and improving scalability [5]. AI-based modules enhance security through anomaly detection and validator prediction, while lightweight cryptography enables fast, energy-efficient authentication

Email addresses: chimesandra@yahoo.com (Amadi Chimeremma Sandra), taesoo.jun@kumoh.ac.kr (Taesoo Jun)

Table 1: Innovation Strategies for Blockchain in AIVs

Technique	Security Benefit	Speed Benefit	Scalability Benefit	Limitations
Hybrid Consensus (PBFT + PoS/PoA)	Prevents malicious nodes; strong trust	Sub-200 ms local consensus	Efficient global synchronization	PBFT overhead in very large networks
Edge-Blockchain	Local data authentication; fewer single points of failure	Reduced propagation delay at RSUs	Tiered edge–cloud design for dense traffic	Requires dense RSU deployment and maintenance
AI-Augmented Security	Detects Sybil/replay attacks in real time	Predictive validator selection reduces delays	Adapts to growing network size dynamically	Complexity of AI models; risk of false positives
Lightweight Cryptography	Secures V2V/V2I with low-cost primitives	Fast authentication, low computational overhead	Supports large-scale vehicular data exchange	Post-quantum schemes still in early stages

for embedded systems [6]. Collectively, these strategies demonstrate that the trilemma can be managed through layered, intelligence driven architectures. Table 1 summarizes their effects across trilemma dimensions.

3. Case Studies: Urban Intersection and Highway Platooning

In dense urban intersections, over 200 AIVs exchange safety data through a tiered blockchain where local PBFT consensus enables sub-200 ms collision-avoidance decisions, supported by AI-driven anomaly detection and validator prediction for enhanced trust and scalability [7]. In contrast, highway platooning employs localized cluster-based consensus and AI-assisted validator selection to maintain secure, real-time coordination across high-speed convoys with 100–150 ms latency, achieving reliable synchronization and fault resilience [8]. Figure 2 compares both scenarios, illustrating how blockchain and AI jointly address the trilemma of security, speed, and scalability in dynamic AIV environments.

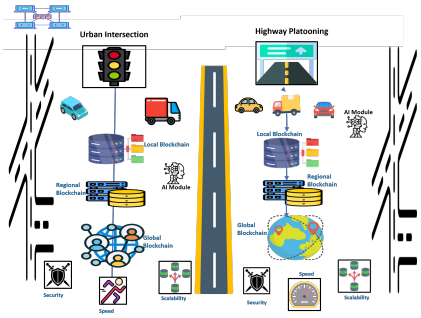

Figure 2: Blockchain trilemma in AIVs; contrasting two scenarios of urban intersection and highway intersection.

4. Challenges and Future Research

The blockchain trilemma limits AIV scalability and responsiveness, as hardware constraints, latency–security trade-offs, energy overhead, and interoperability gaps hinder real-time, secure communication under sub-200 ms safety demands. Future work should focus on quantum-safe cryptography, 6G-enabled networks, adaptive consensus, and AI-assisted hierarchical architectures to balance security, speed, and scalability in next generation intelligent mobility systems.

5. Conclusion

This study shows that balancing security, speed, and scalability through hybrid consensus, edge architectures, AI-augmented security, and lightweight cryptography enables sub-200 ms, scalable blockchain performance in AIVs, demonstrating that the key to future-proof intelligent transportation lies in managing rather than eliminating the blockchain trilemma.

6. Acknowledgment

This work was supported in part by IITP (MSIT) under the Innovative Human Resource Development for Local Intellectualization (IITP-2025-RS-2020-II201612; 34%) and the ITRC program (IITP-2025-RS-2024-00438430; 33%), and by the NRF Basic Science Research Program (Ministry of Education, 2018R1A6A1A03024003; 33%).

References

[1] J. L. López-Ramírez, D. Jimenez-Mendoza, J. M. Benitez-Quintero, E. G. Avina-Bravo, G.-H. D. Asael, A.-C. J. Gabriel, et al., An integrated blockchain framework for secure autonomous vehicle communication system, Information 16 (7) (2025) 557.

[2] G. A. Al-Kafi, G. Ali, S. Reno, Rewriting blockchain: A hybrid consensus that defeats the trilemma paradox, Computers and Electrical Engineering 126 (2025) 110494.

[3] S. Mssassi, A. Abou El Kalam, The blockchain trilemma: A formal proof of the inherent trade-offs among decentralization, security, and scalability, Applied Sciences 15 (1) (2024) 19.

[4] R. Kakkar, R. Gupta, S. Agrawal, S. Tanwar, R. Sharma, Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5g, Journal of Information Security and Applications 67 (2022) 103179.

[5] R. Rathore, P. Kaushik, S. S. Sikarwar, H. Joshi, A. K. Mishra, Y. Hudda, Intelligent transportation systems make use of fog and edge computing for navigation, in: 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI), Vol. 2, 2024, pp. 1–6. doi:10.1109/IATMSI60426.2024.10502525.

[6] M. Sun, Multi-sensor data fusion and management strategies for robust perception in autonomous vehicles, Nuvern Applied Science Reviews 8 (10) (2024) 59–68.

[7] S. Srivastava, D. Agarwal, B. K. Chaurasia, M. Adhikari, Blockchain-based trust management for data exchange in internet of vehicle network, Multimedia Tools and Applications 84 (8) (2025) 4837–4855.

[8] N. Yang, C. Tang, T. Zong, Z. Zeng, Z. Xiong, D. He, Ric-sda: A reputation incentive committee-based secure conditional dual authentication scheme for vanets, IEEE Transactions on Mobile Computing.