A QUEUE-ENABLED CONSORTIUM BLOCKCHAIN ARCHITECTURE FOR LOW-LATENCY V2V COMMUNICATION

Şükrü Okul[1] and Fatih Keleş[2]

[1]TÜBİTAK BİLGEM, Kocaeli, Türkiye
sukru.okul@tubitak.gov.tr
[2]Department of Computer Engineering, Istanbul University Cerrahpasa, Istanbul
fkeles@iuc.edu.tr

ABSTRACT

Secure and low-latency communication is a fundamental requirement for Vehicle-to-Vehicle (V2V) networks operating in highly dynamic environments. Existing vehicular communication architectures often rely on centralized infrastructure or computationally expensive blockchain mechanisms, which limits their applicability in real-time scenarios. This paper introduces a decentralized V2V communication architecture based on a consortium blockchain integrated with the Proof of Authority (PoA) consensus mechanism.

The proposed system removes dependency on roadside infrastructure and delegates transaction validation to authorized consortium nodes. To address congestion and message loss under high traffic conditions, a queue-based transaction pool is employed. Vehicle identities and message integrity are protected using cryptographic mechanisms without introducing excessive processing overhead.

Experimental evaluations demonstrate that the proposed architecture achieves stable and low-latency performance under high transaction arrival rates. The results indicate that combining a permissioned blockchain with queue-based transaction management provides an effective balance between security and performance for next-generation vehicular networks.

KEYWORDS

Vehicular Networks, Consortium Blockchain, Proof of Authority, Queue-Based Transaction Management, Low-Latency Communication

1. INTRODUCTION

Vehicle-to-Vehicle (V2V) communication plays a critical role in intelligent transportation systems by enabling real-time exchange of safety and traffic-related information. However, ensuring secure, reliable, and low-latency communication in highly mobile vehicular environments remains a challenging task. Frequent topology changes, high message volumes, and strict timing requirements limit the effectiveness of traditional centralized communication models [1].

Recent research has increasingly explored blockchain-based solutions to address trust, security, and data integrity issues in vehicular networks [2,3]. Lightweight blockchain frameworks and permissioned ledger systems have been proposed to reduce computational overhead while maintaining decentralized control. Nevertheless, many of these approaches either rely on roadside infrastructure or focus primarily on authentication and privacy preservation, leaving performance degradation and message loss insufficiently addressed [4].

Public blockchain solutions, although fully decentralized, suffer from high latency and resource consumption, making them unsuitable for time-sensitive V2V applications [5]. Conversely, private blockchain architectures often introduce centralized control, which contradicts the fundamental requirements of distributed vehicular environments. Consortium blockchain models have emerged as a promising alternative by offering a balance between decentralization and efficiency [6].

Recent studies also highlight that transaction congestion and queue buildup are major contributors to performance degradation in blockchain-enabled vehicular systems, particularly under high traffic loads [7]. Despite this observation, explicit queue management mechanisms are rarely integrated into consortium blockchain-based V2V architectures.

Motivated by these limitations, this study proposes a consortium blockchain-based V2V communication architecture that integrates the Proof of Authority (PoA) consensus mechanism with a queue-based transaction pool. The proposed design aims to ensure data integrity, prevent message loss, and maintain low latency without relying on roadside infrastructure. Experimental results demonstrate that the proposed approach achieves stable performance under high transaction arrival rates, making it suitable for next-generation vehicular communication systems.

2. LITERATURE REVIEW

Recent studies have explored blockchain-based solutions for enhancing security, privacy, and performance in vehicular communication networks. Ilyas et al. proposed a lightweight consortium blockchain framework with certificateless conditional privacy protection for VANETs, achieving robust security and reduced computational overhead while preserving vehicle identity privacy [8].

Another line of work investigates decentralized blockchain architectures tailored for vehicular environments. A recent study emphasizes distributed consensus and secure data management to address scalability and network reliability in high-mobility scenarios [9].

Moreover, vehicle network-based consensus algorithms have been proposed to reduce transaction latency and increase throughput in vehicular blockchain systems. These approaches utilize optimized consensus mechanisms within permissioned blockchain environments to satisfy real-time communication requirements [10].

Despite these advances, existing studies often focus either on privacy-preserving protocols or alternative consensus strategies, without explicitly integrating queue-based transaction handling mechanisms into consortium blockchain architectures. In contrast, the proposed approach combines a PoA-based consortium blockchain with a queue-managed transaction pool to address message loss and performance degradation under high traffic conditions, while eliminating dependency on roadside units.

3. SYSTEM ARCHITECTURE AND METHODOLOGY

This section presents the proposed blockchain-based architecture designed for secure and efficient Vehicle-to-Vehicle (V2V) communication. The system leverages a consortium blockchain infrastructure combined with the Proof of Authority (PoA) consensus mechanism and a queue-based transaction pool to address security and performance challenges in highly dynamic vehicular environments.

Unlike infrastructure-dependent solutions reported in recent consortium blockchain-based VANET studies [6,8], the proposed architecture eliminates the use of roadside units and relies solely on authorized consortium nodes interconnected via internet connectivity.

3.1 System Components

The proposed system consists of three main components: vehicles, consortium nodes, and a transaction pool. Vehicles exchange safety and status messages, consortium nodes validate transactions and maintain the blockchain ledger, and the transaction pool regulates transaction flow.

3.2 Vehicle Enrollment Procedure

Each vehicle completes an enrollment process by submitting a registration request to the nearest consortium node. The system generates a public–private key pair and a unique hash-based identity, which is recorded in the blockchain and shared among authorized nodes, preventing unauthorized network participation [8].

3.3 Message Transmission and Verification

Verification requests are forwarded to the transaction pool and assigned to available consortium nodes. Identity verification, Merkle root validation, and cryptographic hash checks ensure message integrity before block creation.

3.4 Queue-Based Transaction Pool

Incoming transactions are processed through execution, ordering, and validation stages. This queue-based mechanism mitigates congestion and ensures stable performance under high traffic conditions.

3.5 Consensus Mechanism and Complexity

PoA consensus enables fast validation by trusted nodes, avoiding computationally expensive mining. Vehicle enrollment exhibits constant-time complexity, while message verification operates in logarithmic time, ensuring scalability in high-mobility environments.

4. EXPERIMENTAL SETUP AND RESULTS

Experiments were conducted using Docker-based virtualization with isolated consortium nodes. Synthetic V2V traffic was generated with 100 concurrent messages and a transaction arrival rate of 70 transactions per second. Table 1 summarizes the experimental configuration and system parameters used during the performance evaluation.

Table 1. Experimental Configuration Parameters

Parameter	**Value**
Blockchain Type	Consortium Blockchain
Consensus Mechanism	Proof of Authority (PoA)
Transaction Pool	Queue-Based
Number of Concurrent Msgs	100
Transaction Arrival Rate	70 tx/s
Execution Environment	Docker Containers
Physical Machine	Intel i5, 8 GB RAM

Performance metrics include average waiting time and processing delay across execution, ordering, and validation stages. Results closely follow analytical queueing models, confirming the effectiveness of explicit queue management.

Table 2. Average Processing Time per Transaction Stage (ms)

Stage / Nodes	**5 Nodes**	**7 Nodes**	**15 Nodes**	**21 Nodes**
Execution Stage	3.60	3.52	3.25	2.47
Ordering Stage	8.60	8.51	8.11	7.16
Validation Stage	2.78	2.65	2.29	1.98
Total Avg. Waiting Time (ms)	14.98	14.68	13.65	11.61

The average processing time measured at each transaction stage for different consortium sizes is presented in Table 2. As shown in Table 2, increasing the number of consortium nodes results in a gradual reduction in total waiting time, confirming the scalability of the proposed architecture. Compared to recent lightweight permissioned blockchain frameworks proposed for vehicular and IoT systems [8,9], the proposed architecture achieves competitive or lower latency without additional infrastructure, demonstrating improved system stability under high traffic conditions.

5. CONCLUSION AND FUTURE WORK

This paper presented a consortium blockchain-based architecture for secure and efficient V2V communication. By integrating PoA consensus with a queue-based transaction pool, the system achieves low latency and prevents message loss without roadside infrastructure. Experimental results confirm stable performance aligned with theoretical expectations. Future work will extend the system to multi-host environments and evaluate resilience against advanced attack scenarios and realistic vehicular mobility models.

REFERENCES

[1] M. S. Sheikh, J. Liang and W. Wang, (2019) “A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs)”, Sensors, Vol. 19, No. 16, Article 3589.

[2] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, (2017) “Blockchain: A Distributed Solution to Automotive Security and Privacy”, IEEE Communications Magazine, Vol. 55, No. 12, pp. 119–125.

[3] A. Reyna, C. Martín, J. Chen, E. Soler and M. Díaz, (2018) “On Blockchain and Its Integration with IoT: Challenges and Opportunities”, Future Generation Computer Systems, Vol. 88, pp. 173–190.

[4] H. Luo, X. Yang, J. Duan and H. Yu, (2023) “ESIA: An Efficient and Stable Identity Authentication Scheme for Internet of Vehicles”, IEEE Transactions on Vehicular Technology.

[5] S. Nakamoto, (2008) “Bitcoin: A Peer-to-Peer Electronic Cash System” Technical Report, https://bitcoin.org/bitcoin.pdf

[6] X. Zhang and X. Chen, (2019) “Data Security Sharing and Storage Based on a Consortium Blockchain in Vehicular Ad Hoc Networks”, IEEE Access, Vol. 7, pp. 58241–58254.

[7] M. F. Neuts, (1981) Matrix-Geometric Solutions in Stochastic Models: An Algorithmic Approach, Johns Hopkins University Press.

[8] N. Ilyas, M. Ahmad, M. A. Khan et al., (2024) “A Lightweight Consortium Blockchain-Enabled Secured VANET with Conditional Privacy Preservation”, PLoS ONE, Vol. 19, No. 4.

[9] S. Chen, J. Wu, H. Lin, W. Chen and Z. Zheng, (2019) “A Secure and Efficient Blockchain-Based Data Trading Approach for Internet of Vehicles”, IEEE Transactions on Vehicular Technology, Vol. 68, No. 9, pp. 9110–9121.

[10] X. Yang, H. Luo, J. Duan and H. Yu, (2022) “Ultra-Reliable and Low-Latency Authentication Scheme for Internet of Vehicles Based on Blockchain”, Proceedings of IEEE INFOCOM Workshops, pp. 1–5.