A Study on Blockchain Sharding for Trust Model in IoV

Mahalinoro Razafimanjato, Siddiqa Ayesha, Mahnoor Ajmal, Deepak Singh, Dongkyun Kim

School of Computer Science and Engineering, Kyungpook National University, Republic of Korea

{mahaly, asiddiqa, mahnoor.ajmal, deepak.singh, dongkyun}@knu.ac.kr

Abstract

The Internet of Vehicles (IoV) enables real-time communication among vehicles, roadside units, and road infrastructure but remains vulnerable to malicious behavior due to a lack of established trust among entities. Blockchain-based trust management systems address this by evaluating the credibility of messages and monitoring vehicle behavior. However, existing solutions struggle with low throughput. To overcome this, we propose a blockchain-based sharding trust model that partitions the network for parallel processing. We also integrate a trust evaluation mechanism with an incentive-based system to detect malicious nodes. Simulation results confirm our approach significantly improves throughput and enhances trust computation.

Ⅰ. Introduction

IoV is an inter-vehicular network enabling real-time communication and data exchange between various entities and surrounding environments, such as vehicles, roadside units (RSUs), and traffic infrastructure to enhance driving safety, traffic efficiency, and infotainment services for drivers and passengers [1]. Due to its high mobility and dynamic topology, IoV entities often lack established trust, creating opportunities for malicious entities to inject false messages or tamper with message content, severely impacting network reliability and road safety.

Trust management systems mitigate these threats by evaluating message credibility and vehicle trustworthiness based on historical interactions and contextual information [2]. However, traditional trust management systems are often centralized, raising concerns about scalability and single points of failure. Blockchain addresses these limitations by offering decentralized, transparent, and tamper-resistant trust management solutions [3]. Several studies [4-5] have explored integrating blockchain with trust management in vehicular networks, primarily as a storage infrastructure for trust data. However, existing solutions struggle with low scalability due to restricted transaction throughput and high consensus latency during peak traffic conditions, making real-time trust computation challenging in a dynamic IoV environment.

In order to address the challenges mentioned above, we propose a blockchain-based sharding vehicular trust management system. This work leverages blockchain sharding by partitioning the network into geographical regions and distributing trust-related transactions across shards, enabling parallel processing to achieve higher throughput. To mitigate malicious nodes and messages within the network, we introduce a trust model that evaluates the credibility of messages and vehicles with a reward and punishment mechanism to ensure reliable trust computation and incentivize honest behavior.

Ⅱ. Proposed Scheme

Fig. 1 illustrates the system model and overall workflow of our proposed blockchain-based trust management model. This model includes vehicles as minimally trusted mobile nodes contributing to traffic data and trust computation and RSUs as fully trusted static nodes with sufficient resources to manage transactions, perform intra- and inter-shard consensus, and maintain the shard ledger.

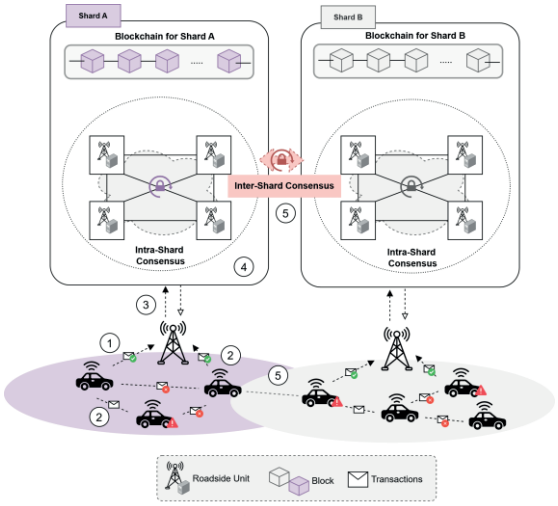

Fig. 1: ①,② Local Message Credibility Evaluation ③ Intra-shard Trust Aggregation ④ PBFT-based Intra-shard Consensus Mechanism & Trust Update ⑤ Relay-based Intra-shard Consensus & Transaction.

The network is geographically partitioned into shards (e.g., Shard A and Shard B), each managed by a set of RSUs responsible for verifying and storing local trust transactions. Vehicles are assigned to shards based on their location, and intra-shard consensus is achieved using PBFT. When vehicles move across shard boundaries, a relay mechanism transfers trust data between shards, ensuring

consistency and atomicity. Our trust model evaluates message credibility based on sender reputation and proximity, aggregated locally by vehicles and globally by RSUs within each shard. Vehicles providing truthful reports and ratings receive increased trust scores, while malicious nodes are penalized accordingly with decreased trust scores.

Ⅲ. Performance Evaluation

To evaluate our proposed trust model scheme, we set up our simulation using SUMO to generate an urban traffic scenario in an area around Daegu, South Korea, Python for trust logic, BlockEmulator [6] to simulate sharding. Detailed simulation parameters are summarized in Table I.

Table I: Simulation Parameters

Parameters	Value
Number of RSUs	16
Number of Vehicles	100-400
Initial Trust Score	0.7¬0.8
Block Interval	1s
Block Size	1MB
Number of Shards	2/4/8
Delay	10ms
Jitter	5ms
w	0.0008
τ , Θ	0.6
λ , δ	0.05

As seen in Fig. 2, the trust model effectively penalizes malicious vehicles, as trust scores gradually decline over time while genuine vehicles consistently provide accurate messages and truthful ratings, leading to a steady increase in their trust scores. Fig. 3 depicts the significant improvement of sharding compared to non-sharded trust models. The transaction throughput increases from 60 TPS (non-sharded s=1) to over 200 TPS with 8 shards, and confirmation latency drops from ~8s to ~3s. It is important to note that the actual TPS may vary depending on network latency, block size, and hardware specifications.

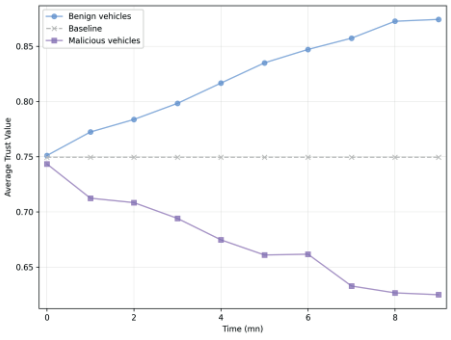

Fig. 2 Trust Score Variation Over Time

Ⅳ. Conclusion

In this paper, we proposed a blockchain-based sharding trust model for IoV to address the performance limitations in existing solutions. By leveraging sharding, our system enables parallel trust transaction processing, significantly improving throughput and reducing confirmation delays. We also integrated a trust computation mechanism to detect malicious vehicles. Simulation results confirm the effectiveness of our proposed scheme. Future work will explore adaptive sharding strategies to overcome static shard limitations, handle hot shard congestion, and minimize cross-shard overhead in dynamic vehicular environments.

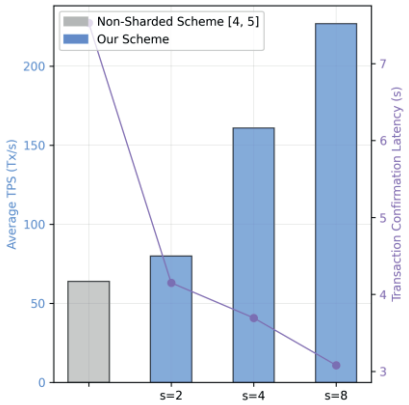

Fig. 3 Average Transaction Throughput and Transaction Confirmation Latency Comparison

ACKNOWLEDGMENT

This research has supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT), (NRF-2022R1A2C1003620).

REFERENCES

[1] Y. Wang, H. Zen, M. F. M. Sabri, X. Wang, and L. C. Kho, “Towards strengthening the resilience of iov networks—a trust management perspective,” Future Internet, vol. 14, no. 7, p. 202, 2022.

[2] A. Mahmood, Q. Z. Sheng, S. A. Siddiqui, S. Sagar, W. E. Zhang, H. Suzuki, and W. Ni, “When trust meets the internet of vehicles: Opportunities, challenges, and future prospects,” in 2021 IEEE 7th International Conference on Collaboration and Internet Computing (CIC), pp. 60- 67, IEEE, 2021.

[3] W. Ruan, J. Liu, Y. Chen, S. M. N. Islam, and M. Alam, “Trust management model for secure internet of vehicles,” Encyclopedia, 2024. Accessed: 26 November 2024.

[4] F. Lin, Y. Peng, T. Cui, X. Huang, and Q. Chen, “Blockchain based content sharing management in vanets,” in 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), pp. 1- 5, IEEE, 2021

[5] M. Firdaus, S. Rahmadika, and K.-H. Rhee, “Decentralized trusted data sharing management on internet of vehicle edge computing (iovec) networks using consortium blockchain,” Sensors, vol. 21, no. 7, p. 2410, 2021

[6] H. Huang, G. Ye, Q. Yang, Q. Chen, Z. Yin, X. Luo, J. Lin, J. Zheng, T. Li, and Z. Zheng, “Blockemulator: An emulator enabling to test blockchain sharding protocols,” IEEE Transactions on Services Computing, 2025.