Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 2, pp 1-5, February 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.202001
Available Online at https://www.jaiet.com

The Role of Blockchain in Securing the Internet of Vehicles: A Comprehensive Review

D. Dinesh Raja

Department of Electronics and Communication Engineering, Sri Shakthi Institute of Engineering and Technology, Coimbatore, India

Abstract: The rapid evolution of the Internet of Vehicles (IoV) has enabled intelligent transportation systems through real-time vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communication. However, the highly distributed and dynamic nature of IoV networks introduces significant challenges related to security, privacy, data integrity, and trust management. Centralized architectures are particularly vulnerable to single points of failure, cyberattacks, data manipulation, and unauthorized access. In this context, Blockchain technology has emerged as a promising decentralized solution capable of enhancing security and transparency within vehicular networks. This comprehensive review examines the role of blockchain in addressing critical IoV security concerns, including authentication, secure data sharing, intrusion detection, privacy preservation, and trust evaluation. The study analyzes various blockchain architectures—public, private, and consortium networks—and evaluates their suitability for vehicular environments. It further explores the integration of smart contracts, consensus mechanisms, and cryptographic protocols to ensure secure communication among vehicles and infrastructure nodes. Additionally, the review highlights current research trends, scalability limitations, latency challenges, and energy efficiency concerns associated with blockchain deployment in real-time vehicular systems. The findings indicate that blockchain-based frameworks significantly improve data integrity, decentralized trust management, and resilience against malicious attacks. However, practical implementation requires optimization strategies to overcome computational overhead and network delay constraints. This review provides a structured understanding of blockchain-enabled IoV security models and outlines future research directions aimed at developing scalable, efficient, and privacy-preserving vehicular communication systems.

Keywords: Blockchain; Internet of Vehicles (IoV); Vehicular Ad Hoc Networks (VANETs); Smart Contracts; Distributed Ledger Technology (DLT); Cybersecurity; Privacy Preservation.

I. INTRODUCTION

The rapid advancement of intelligent transportation systems has led to the emergence of the Internet of Vehicles (IoV), a network paradigm that enables communication among vehicles, roadside infrastructure, pedestrians, and cloud services. IoV facilitates real-time data exchange to improve road safety, traffic efficiency, and autonomous driving capabilities. Through Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) communication, IoV enhances situational awareness and decision-making in transportation systems.

However, the decentralized and highly dynamic nature of vehicular networks introduces serious challenges in terms of data security, privacy preservation, authentication, and trust management. Malicious nodes may inject false information, launch denial-of-service attacks, or compromise communication integrity. To address these vulnerabilities, Blockchain technology has emerged as a promising solution due to its decentralized, tamper-resistant, and transparent characteristics. This review paper explores how blockchain can enhance IoV security, improve trust management, and enable secure data sharing across vehicular networks.

II. PROBLEM STATEMENT

Despite the promising benefits of IoV, its large-scale deployment faces critical security and scalability concerns. Traditional centralized architectures are prone to single points of failure and cannot efficiently manage trust among highly mobile nodes. Vehicles continuously generate massive volumes of data, including traffic updates, sensor readings, and emergency alerts. Ensuring the authenticity and integrity of this data in real time is challenging.

Moreover, IoV environments demand ultra-low latency communication, which conflicts with the computational overhead of conventional security mechanisms. Privacy issues

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 2, pp 1-5, February 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.202001
Available Online at https://www.jaiet.com

also arise as vehicles transmit location and identity-related information. Therefore, there is a need for a decentralized framework capable of secure message validation, transparent data management, and robust authentication without compromising performance. Blockchain offers a distributed trust mechanism that can address these limitations while maintaining data immutability and transparency.

III. BACKGROUND STUDY

The integration of blockchain technology into the Internet of Vehicles (IoV) is an emerging research area aimed at addressing longstanding trust, security, and data integrity issues in connected vehicular environments. One of the foundational comprehensive surveys in this domain was presented by Muhammad Baqer Mollah et al., who explored the application of blockchain to support the information exchange needs of IoV towards realizing the vision of intelligent transportation systems (ITS). Their work emphasizes that IoV, as a participatory data exchange platform between vehicles, infrastructure, and sensors, necessitates decentralized and transparent mechanisms to provide secure, immutable, and automated data sharing that overcomes centralized architecture limitations and enhances safety and interoperability within ITS ecosystems.

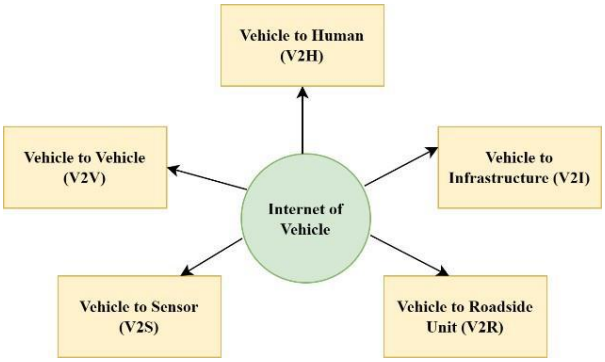

Figure 1: Internet of Vehicle Communication

Expanding on application-oriented perspectives, Chao Wang et al. reviewed how blockchain can be implemented in IoV to improve architecture, security, privacy, and data management. Their survey categorizes deployment strategies across multiple aspects of IoV operations, including how decentralized ledgers can replace centralized authorities for secure authentication, data integrity, and transparent vehicle coordination. It highlights the key advantages of blockchain — such as decentralization, immutability, and enhanced confidentiality — which collectively contribute to strengthening vehicular trust mechanisms.

Focusing specifically on authentication, Sohail Abbas et al. provide one of the most detailed reviews of blockchain-based authentication mechanisms in IoV and traditional Vehicular Ad Hoc Networks (VANETs). Their work outlines a taxonomy of authentication schemes, analyzing different techniques, network models, and real-world threats that these schemes aim to counteract, such as impersonation attacks and message tampering. The review further discusses how permissioned and consortium blockchain models can support secure identity verification, secure routing, and privacy preservation by leveraging cryptographic and distributed consensus protocols.

Privacy is another critical dimension explored by Wendong Chen et al., who surveyed blockchain-based privacy protection strategies tailored for IoV systems. Their review classifies privacy concerns into identity, location, and data privacy, revealing that most existing blockchain solutions primarily target identity privacy while also integrating techniques such as pseudonymization and permissioned ledger designs to address broader privacy challenges. They show that popular blockchain platforms such as Hyperledger Fabric and Ethereum are frequently adopted in these solutions, often in hybrid configurations, to achieve different levels of privacy and performance trade-offs.

More recent surveys focus on specific facets such as trust management. A systematic review on blockchain-based trust management systems highlights how immutability and decentralized trust computation can enhance reliability and integrity in IoV communication. It classifies approaches by trust computation methods, including AI-driven models and optimized consensus protocols, and discusses integration with emerging technologies like 5G/6G networks and federated learning for greater scalability and adaptability in IoV environments.

Other research has examined the synergy between blockchain and edge computing in vehicular networks, recognizing that edge resources can mitigate latency and bandwidth challenges while supporting decentralized validation and data distribution among IoV participants. This body of work identifies both opportunities and limitations in combining edge intelligence with blockchain's distributed ledger, reinforcing the importance of architectural design choices in real-time IoV scenarios.

Collectively, these studies establish that blockchain's decentralized consensus mechanisms, cryptographic integrity,

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 2, pp 1-5, February 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.202001
Available Online at https://www.jaiet.com

and transparent transaction history can significantly enhance security, privacy, and trust management in IoV systems. Nevertheless, the literature also identifies persistent challenges — including consensus protocol overhead, scalability under high-mobility networks, and integration with heterogeneous communication technologies — that remain active areas of research. Future work is increasingly focusing on hybrid models, lightweight consensus algorithms, and cross-layer optimizations to address performance trade-offs without compromising security.

Internet of Vehicles

The Internet of Vehicles extends the concept of the Internet of Things (IoT) into vehicular environments by connecting smart vehicles, roadside units (RSUs), and cloud platforms. IoV integrates communication technologies such as Dedicated Short Range Communication (DSRC), 5G, and edge computing to enable seamless information exchange. Applications include collision avoidance, traffic congestion control, autonomous navigation, and infotainment services. However, due to high node mobility and open wireless channels, IoV networks are vulnerable to spoofing, Sybil attacks, data tampering, and identity theft. Traditional Vehicular Ad Hoc Networks (VANETs) rely on centralized certification authorities, which may become bottlenecks or targets for cyberattacks.

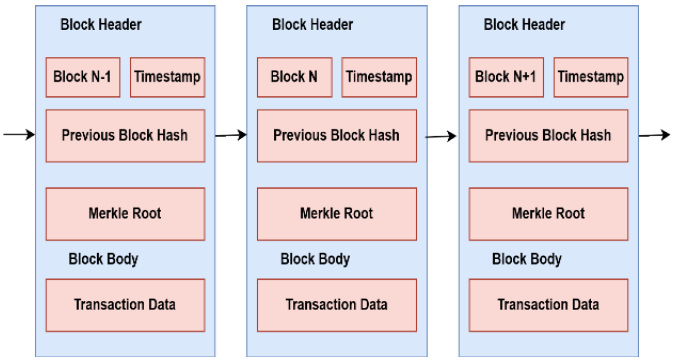

Figure 2: Data Structure of Blocks

Blockchain

Blockchain is a distributed ledger technology that records transactions in a decentralized and immutable manner. Each block contains a cryptographic hash of the previous block, ensuring data integrity and resistance to tampering. Consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) enable agreement among distributed nodes without centralized control. Smart contracts further automate transaction validation processes. In IoV applications, blockchain can provide decentralized identity management, secure message authentication, and transparent trust evaluation among vehicles and infrastructure nodes.

IV. METHODOLOGY

This comprehensive review analyzes existing research on blockchain-enabled IoV systems and proposes a structured framework for integrating blockchain into vehicular communication networks. The methodology includes identifying IoV security requirements, examining blockchain architectures suitable for vehicular environments, and evaluating performance trade-offs.

A layered architecture model is considered, where vehicles act as lightweight nodes while roadside units and edge servers participate in blockchain validation processes. The study evaluates public, private, and consortium blockchain models to determine their suitability for real-time vehicular communication. Emphasis is placed on scalability optimization techniques such as sharding, off-chain storage, and hybrid blockchain-edge integration.

V. INTEGRATION OF IoV AND BLOCKCHAIN

Integration of IoV and Blockchain

The integration framework involves embedding blockchain nodes within roadside infrastructure and cloud servers, while vehicles function as transaction initiators. When vehicles generate traffic or safety messages, the data is encrypted and transmitted to nearby RSUs. These RSUs validate and record transactions onto the blockchain ledger. This decentralized approach eliminates reliance on a single trusted authority and enhances resilience against cyberattacks.

Message Validation in IoV with Blockchain

Blockchain enhances message validation by using digital signatures and cryptographic hashing techniques. Each vehicular message is signed using a private key and verified using a public key infrastructure integrated with blockchain. Once validated, the message is stored in an immutable ledger, preventing alteration or replay attacks. Smart contracts automate trust evaluation by assigning reputation scores to vehicles based on historical behavior. This mechanism effectively mitigates malicious data injection and Sybil attacks.

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 2, pp 1-5, February 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.202001
Available Online at https://www.jaiet.com

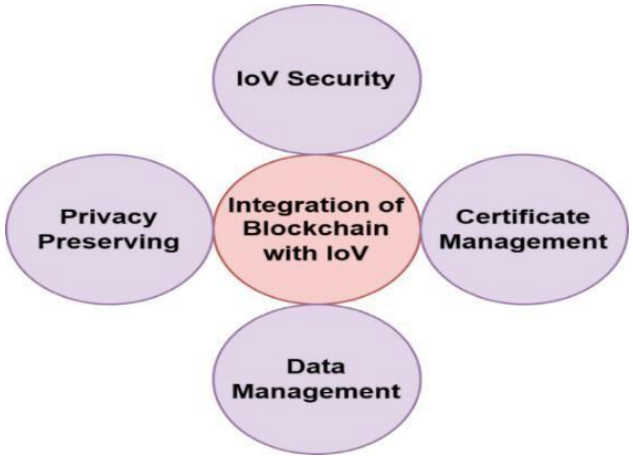

Figure 3: Integration of Blockchain with IoV

Data Management in IoV with Blockchain

Efficient data management is critical due to the high data generation rate in IoV systems. Instead of storing large datasets directly on-chain, off-chain storage solutions such as InterPlanetary File System (IPFS) are combined with blockchain to maintain scalability. Only metadata and hash values are stored on the blockchain, ensuring integrity verification without excessive storage overhead. Edge computing further reduces latency by processing data closer to vehicles before blockchain validation.

VI. RESULTS AND EVALUATION

The review of existing blockchain-IoV frameworks indicates significant improvements in trust management, data integrity, and resistance to cyberattacks compared to traditional centralized systems. Blockchain-based authentication schemes reduce the risk of identity spoofing and unauthorized access. Simulation studies reported in the literature demonstrate enhanced security performance with acceptable latency when lightweight consensus algorithms such as PBFT are used.

However, challenges remain regarding computational overhead, energy consumption, and network scalability. Public blockchains with heavy consensus mechanisms may introduce delays incompatible with real-time vehicular communication. Hybrid and consortium blockchain models show better performance in IoV scenarios by balancing decentralization and efficiency.

VII. FUTURE SCOPE

Future research should focus on optimizing consensus mechanisms specifically designed for high-mobility vehicular environments. Integration with 6G communication networks and AI-based anomaly detection systems can further enhance IoV security. Federated learning combined with blockchain may enable privacy-preserving collaborative intelligence among vehicles. Additionally, large-scale real-world implementation and cross-border vehicular communication standardization remain open research areas.

VIII. CONCLUSION

This review highlights the transformative potential of blockchain technology in securing the Internet of Vehicles. By providing decentralized trust management, immutable data storage, and automated validation through smart contracts, blockchain addresses key security and privacy challenges in IoV networks. Although scalability and latency issues require further optimization, blockchain-enabled frameworks offer a promising direction for building secure, transparent, and intelligent transportation ecosystems. Continued research and technological advancements will play a crucial role in realizing fully decentralized and secure vehicular communication infrastructures.

REFERENCES

[1] Mollah, M. B., et al. (2020). Blockchain for the Internet of Vehicles towards Intelligent Transportation Systems: A Survey. arXiv:2007.06022.

[2] Wang, C., Cheng, X., Li, J., He, Y., & Xiao, K. (2021). A survey: applications of blockchain in the Internet of Vehicles. EURASIP Journal on Wireless Communications and Networking.

[3] Abbas, S., Abu Talib, M., Ahmed, A., Khan, F., Ahmad, S., & Kim, D.-H. (2021). Blockchain-Based Authentication in Internet of Vehicles: A Survey. Sensors, 21(23), 7927.

[4] Chen, W., Wu, H., Chen, X., & Chen, J. (2022). A Review of Research on Privacy Protection of Internet of Vehicles Based on Blockchain. J. Sens. Actuator Netw., 11(4), 86.

[5] Kumar, S., et al. (2021). A survey on the blockchain techniques for the Internet of Vehicles security. Transactions on Emerging Telecommunications Technologies.

[6] Blockchain-based trust management systems in the Internet of Vehicles: A comprehensive survey. (2025). ICT Express.

[7] Dorri, A., et al. (2017). Blockchain for IoT security and

Journal of Artificial Intelligence and Emerging Technologies
Volume 2, Issue 2, pp 1-5, February 2025
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2025.202001
Available Online at https://www.jaiet.com

privacy. IEEE Internet of Things Journal.

[8] Sharma, P. K., et al. (2018). Blockchain-based distributed framework for vehicular networks. IEEE Access.

[9] Lu, Y., et al. (2019). Blockchain in vehicular networks: A survey. IEEE Communications Surveys & Tutorials.

[10] Zhang, Y., et al. (2018). Blockchain-based secure data sharing in vehicular networks. IEEE Transactions on Intelligent Transportation Systems.

[11] Singh, M., & Kim, S. (2019). Blockchain-based intelligent vehicle data sharing framework. Sensors.

[12] Abbas, F., et al. (2020). Lightweight blockchain framework for IoV security. Future Generation Computer Systems.

Citation of this Article:

D. Dinesh Raja. (2025). The Role of Blockchain in Securing the Internet of Vehicles: A Comprehensive Review. *Journal of Artificial Intelligence and Emerging Technologies (JAIET).* 2(2), 1-5. Article DOI: https://doi.org/10.47001/JAIET/2025.202001

***** End of the Article *****