

BLOCKCHAIN-BASED SECURE DATA COMMUNICATION BETWEEN AUTONOMOUS VEHICLES

Mr Nagesh U B¹, Soniya Katrale², Avinash Mundolli³, B Ranjith Nayak⁴

¹ Faculty, Department of Information Science and Engineering

^{2,3,4} U G Scholar, Department of Information Science and Engineering Alva's Institute Of Engineering And Technology, Karnataka, India

ABSTRACT

Autonomous vehicles are becoming an important part of intelligent transportation systems because they support automated driving, traffic monitoring, and real-time communication between vehicles and in-frastructure systems. However, traditional vehicular communication networks are vulnerable to cyber-attacks, data tampering, spoofing, unauthorized access, and privacy leakage that may affect transportation safety and intelligent driving operations. Blockchain technology provides decentralized and secure communication using distributed ledgers, cryptographic algorithms, and smart contracts that improve trust management, privacy preservation, communication reliability, and secure data sharing in vehicular environments. The integration of blockchain with Artificial Intelligence, Edge Computing, Federated Learning, 5G communication, and Internet of Vehicles technologies further enhances transportation efficiency, cybersecurity, and intelligent traffic management in future smart city environments.

Keyword: Blockchain, Autonomous Vehicles, V2V Communication, Cybersecurity, IoV, Smart Contracts

1. INTRODUCTION

Autonomous vehicles are becoming one of the most advanced technologies in intelligent transportation systems because they improve road safety, reduce human driving errors, and support automated transportation services. These vehicles use advanced sensors, cameras, radar systems, GPS modules, LiDAR devices, and wireless communication technologies to collect and exchange traffic information in real time. Vehicle-to-Vehicle communication allows autonomous vehicles to exchange speed, navigation, and emergency alert information with nearby vehicles, while Vehicle-to-Infrastructure communication supports communication with traffic lights, roadside units, and transportation management systems.

Traditional vehicular communication systems mainly depend on centralized architectures that are vulnerable to cyberattacks, communication failures, and unauthorized access. Attackers may inject fake messages, manipulate navigation information, or perform spoofing attacks that affect intelligent transportation systems and passenger safety. Blockchain technology provides decentralized communication frameworks that improve communication trust, privacy

preservation, tamper-proof data storage, and secure authentication mechanisms in autonomous vehicular networks. The integration of blockchain with intelligent transportation technologies further improves transportation efficiency, decentralized trust management, and cybersecurity in smart city environments.

2. NEED FOR SECURE VEHICULAR COMMUNICATION

Autonomous vehicles continuously exchange sensitive information such as traffic congestion details, emergency alerts, navigation data, weather conditions, and intelligent driving instructions through wireless vehicular communication systems. Since autonomous transportation systems depend heavily on real-time communication, any delay or modification of communication data may create transportation

safety risks and affect intelligent driving decisions. Traditional centralized communication architectures may also experience communication bottlenecks, server failures, and scalability limitations during large-scale transportation operations.

Cybersecurity threats such as spoofing attacks, Sybil attacks, fake message injection, replay

attacks, and Distributed Denial of Service attacks may manipulate vehicular communication systems and create dangerous transportation conditions. Secure vehicular communication is therefore essential for protecting autonomous transportation systems from malicious communication activities. Blockchain technology improves vehicular communication security through encrypted transactions, decentralized authentication, tamper-proof ledgers, and secure distributed trust management that protect connected transportation networks from unauthorized access and communication manipulation.

3. BLOCKCHAIN TECHNOLOGY IN AUTONOMOUS VEHICLES

Blockchain is a decentralized distributed ledger technology that securely records communication transactions in interconnected blocks protected using cryptographic algorithms. Each communication transaction is verified using consensus mechanisms before being added to blockchain ledgers, ensuring transparency, trust management, and tamper-proof data storage. Blockchain networks eliminate the dependency on centralized authorities and improve secure communication between connected autonomous vehicles and transportation infrastructure systems.

In autonomous vehicular networks, blockchain technology supports secure Vehicle-to-Vehicle and Vehicle-to-Infrastructure communication by protecting communication records from unauthorized modifications and cyberattacks. Smart contracts automate transportation operations such as parking management, toll collection, insurance processing, ride-sharing services, and electric vehicle charging systems. Blockchain technology also improves decentralized trust management where connected vehicles can securely verify communication entities without relying on centralized communication authorities, improving intelligent transportation efficiency and cybersecurity.

4. ARCHITECTURE OF BLOCKCHAIN-BASED VEHICULAR NETWORKS

Blockchain-based autonomous vehicular communication systems consist of autonomous vehicles, road-side units, blockchain nodes, cloud servers, edge devices, and intelligent transportation management systems.

Autonomous vehicles continuously exchange information related to road conditions, traffic congestion, accident alerts, navigation updates, and intelligent driving instructions through wireless communication networks. Roadside Units support communication management between vehicles and transportation infrastructure systems while improving real-time communication processing.

Blockchain nodes verify vehicular communication transactions and securely store verified communication records in decentralized distributed ledgers. Edge computing devices process communication data closer to transportation networks to reduce communication latency and improve transportation efficiency. Cloud servers provide large-scale communication storage and intelligent transportation analytics. The combined architecture improves decentralized trust management, communication reliability, secure data sharing, and cybersecurity in intelligent transportation systems.

5. APPLICATIONS OF BLOCKCHAIN IN AUTONOMOUS VEHICLES

Blockchain technology supports secure communication between autonomous vehicles by protecting communication messages from cyberattacks, fake message injection, and unauthorized modifications. Blockchain-enabled authentication systems allow connected vehicles to verify the identity of communication entities securely without depending on centralized authorities. Secure communication improves transportation reliability, intelligent driving performance, and road safety in smart transportation systems.

Blockchain technology is also widely used in intelligent traffic management systems, toll collection services, parking management applications, insurance claim processing, ride-sharing platforms, electric vehicle charging systems, and fleet management services. The integration of blockchain with Internet of Vehicles technologies further improves transportation efficiency, communication transparency, privacy protection, decentralized trust management, and secure autonomous transportation operations in future smart city environments.

6. SECURITY CHALLENGES IN AUTONOMOUS VEHICULAR SYSTEMS

Autonomous vehicular communication systems face several cybersecurity challenges because vehicles continuously exchange large amounts of wireless communication data with nearby vehicles and transportation infrastructure systems. Unauthorized access, spoofing attacks, replay attacks, Distributed Denial of Service attacks, and data tampering attacks may manipulate communication information and affect intelligent driving decisions. Communication failures and malicious attacks may therefore create serious transportation safety risks in autonomous vehicular environments.

Privacy leakage is another major challenge because autonomous vehicles collect sensitive information such as travel history, real-time vehicle location, driving behavior, and passenger communication records. Traditional communication architectures often struggle to protect user privacy and communication integrity during large-scale transportation operations. Blockchain technology improves communication security through encrypted communication frameworks, tamper-proof ledgers, decentralized authentication mechanisms, and distributed trust management that strengthen vehicular communication cybersecurity and privacy preservation.

7. ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN INTEGRATION

Artificial Intelligence plays an important role in intelligent transportation systems by improving autonomous driving operations, transportation analytics, intelligent decision-making, and traffic prediction mechanisms. AI algorithms analyze communication records, traffic congestion data, road conditions, weather updates, and vehicle sensor information to improve transportation efficiency and intelligent driving performance. Machine Learning techniques also support cyberattack detection, accident prediction, and intelligent route optimization in autonomous vehicular networks.

The integration of blockchain with Artificial Intelligence improves secure data sharing, decentralized trust management, communication transparency, and intelligent automation in transportation systems. Blockchain technology securely stores AI training records and

communication information, preventing unauthorized modifications and improving intelligent system reliability. Blockchain-enabled AI systems also improve cyberattack detection, decentralized communication management, and intelligent transportation analytics while supporting secure and efficient autonomous transportation services.

8. EDGE COMPUTING AND BLOCKCHAIN

Edge Computing is an advanced technology that processes communication data closer to vehicular communication networks instead of relying completely on centralized cloud servers. Autonomous vehicles continuously generate massive amounts of communication information from cameras, sensors, radar systems, GPS modules, and intelligent transportation applications. Processing all vehicular communication data through centralized cloud systems may increase communication latency, network congestion, and transportation inefficiency.

Blockchain-enabled Edge Computing systems improve low-latency communication, cybersecurity, communication reliability, and intelligent transportation performance by supporting real-time communication processing near transportation environments. Edge devices such as roadside units and local servers help process communication data quickly and securely while reducing cloud dependency. The integration of blockchain and edge computing therefore improves secure autonomous driving operations, intelligent transportation management, and decentralized communication efficiency in smart transportation systems.

9. INTERNET OF VEHICLES (IOV)

Internet of Vehicles is an intelligent communication framework that connects autonomous vehicles, roadside infrastructure systems, communication devices, traffic management systems, and cloud servers for real-time information sharing and transportation management. IoV technologies improve communication efficiency, intelligent traffic monitoring, road safety, transportation automation, and smart city transportation services through continuous communication between connected transportation entities.

Blockchain technology improves communication security in IoV environments through encrypted

communication mechanisms, decentralized authentication systems, tamper-proof storage frameworks, and distributed trust management. Blockchain-enabled IoV systems improve communication reliability, privacy preservation, secure data sharing, and transportation transparency while protecting connected transportation networks from malicious communication activities. The integration of blockchain and IoV technologies significantly improves intelligent transportation efficiency and cybersecurity in future autonomous transportation systems.

10. ADVANTAGES OF BLOCKCHAIN IN AUTONOMOUS TRANSPORTATION

Blockchain technology improves vehicular communication security by protecting communication transactions using decentralized distributed ledgers and advanced cryptographic algorithms. Secure data sharing improves communication reliability, intelligent transportation efficiency, decentralized trust management, and privacy preservation in autonomous vehicular networks. Blockchain systems also eliminate dependency on centralized authorities, reducing communication bottlenecks and improving communication transparency in intelligent transportation systems.

Another major advantage of blockchain technology is tamper-proof communication storage that improves accountability and prevents unauthorized modification of transportation records. Smart contracts automate transportation services such as parking systems, insurance processing, toll collection, secure payment systems, and ride-sharing applications while reducing operational complexity and improving intelligent automation. Blockchain technology therefore supports secure, decentralized, reliable, and efficient transportation management in smart city environments.

11. CHALLENGES OF BLOCKCHAIN TECHNOLOGY

Although blockchain technology provides several advantages in autonomous transportation systems, multiple technical challenges still exist in blockchain-enabled vehicular communication networks. Scalability is one of the major challenges because autonomous vehicular systems continuously generate massive amounts of

communication data that require secure storage, verification, and processing. Large-scale communication verification may increase computational complexity and communication delay in intelligent transportation systems.

Computational overhead, storage complexity, energy consumption, and infrastructure cost also affect blockchain implementation in autonomous vehicular networks. Consensus mechanisms often require significant processing resources that may reduce communication efficiency in real-time transportation environments. Integration complexity between blockchain systems and existing transportation infrastructures is another important challenge that researchers continue to address for large-scale deployment of secure blockchain-enabled transportation systems.

12. FUTURE RESEARCH DIRECTIONS

Future research mainly focuses on improving blockchain scalability, cybersecurity, communication efficiency, and intelligent transportation performance in autonomous vehicular communication systems. Lightweight blockchain frameworks and efficient consensus algorithms are being developed to support secure low-latency communication and real-time transportation applications. Researchers are also investigating advanced cryptographic techniques to strengthen communication privacy and decentralized trust management in autonomous vehicular networks.

The integration of Artificial Intelligence, Federated Learning, 5G communication, Edge Computing, and Internet of Vehicles technologies will further improve intelligent transportation services and decentralized communication management. Quantum-resistant cryptographic algorithms are also being developed to improve long-term communication security against future cyber threats. Future blockchain-enabled transportation systems are expected to support secure, intelligent, decentralized, and highly efficient autonomous transportation services in future smart cities.

13. CONCLUSION

Blockchain-based secure data communication plays a major role in improving communication reliability, decentralized trust management, privacy preservation, and cybersecurity in autonomous vehicular communication networks.

Blockchain technology provides secure authentication systems, encrypted communication mechanisms, tamper-proof distributed ledgers, and decentralized communication frameworks that strengthen intelligent transportation systems and autonomous driving operations.

The integration of blockchain with Artificial Intelligence, Edge Computing, Federated Learning, In-ternet of Vehicles technologies, and 5G communication significantly improves intelligent

transportation performance and communication efficiency. Although several technical challenges such as scalability, communication latency, and computational overhead still exist, blockchain technology will continue to support the development of secure, reliable, decentralized, and intelligent autonomous transportation systems for future smart city environments.

14. COMPARISON OF TRADITIONAL AND BLOCKCHAIN-BASED COMMUNICATION

Feature	Traditional System	Blockchain-Based System
Architecture	Centralized	Decentralized
Security Level	Moderate	High
Data Tampering Risk	High	Very Low
Trust Management	Central Authority	Distributed Trust
Privacy Protection	Limited	Strong Encryption
Communication Reliability	Moderate	High
Single Point Failure	Present	Eliminated
Authentication Method	Centralized	Decentralized
Transparency	Limited	High
Cyberattack Resistance	Lower	Stronger

REFERENCES

- [1] Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," IEEE Internet of Things Journal, 2019.
- [2] M. Singh and S. Kim, "Blockchain Based Intelligent Vehicular Communication Framework," IEEE Access, 2019.
- [3] T. Alladi, V. Chamola, N. Kumar, and M. Guizani, "Blockchain Applications for Intelligent Transportation Systems," IEEE Communications Magazine, 2020.
- [4] X. Sun, P. Wang, and M. Zhao, "Privacy-Preserving Communication in Vehicular Networks Using Blockchain," IEEE Transactions on Vehicular Technology, 2021.
- [5] S. Sharma, R. Gupta, and P. Singh, "Blockchain-Enabled Secure Communication Framework for Autonomous Vehicles," International Journal of Network Security, 2021.
- [6] Y. Zhang, R. Zheng, and T. J. Lim, "Secure V2V and V2I Communication Using Blockchain Technology," IEEE Communications Magazine, 2019.
- [7] P. Kumar, G. Srivastava, and M. Conti, "Federated Learning for Intelligent Internet of Vehicles Systems," IEEE Network, 2022.
- [8] R. Gupta and S. Kumar, "Decentralized Trust Management in Blockchain-Based Vehicular Networks," IEEE Internet of Things Journal, 2021.
- [9] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Blockchain for Secure and Efficient Data Sharing in Vehicular Edge Computing and Networks," IEEE Internet of Things Journal, 2019.
- [10] K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-Based Efficient Privacy Preserving and Data Sharing Scheme for Vehicular Networks," IEEE Transactions on Vehicular Technology, 2020.
- [11] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet Security Challenges

and Solutions: A Survey,” Vehicular Communications Journal, 2017.

- [12] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Blockchain White Paper, 2008.
- [13] M. Conoscenti, A. Vetro, and J. C. De Martin, “Blockchain for the Internet of Things: A System-atic Literature Review,” IEEE Conference, 2016.
- [14] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, “A Privacy-Preserving Trust Model Based on Blockchain for VANETs,” IEEE Access, 2018.
- [15] Y. Yuan and F. Wang, “Towards Blockchain-Based Intelligent Transportation Systems,” IEEE International Conference on Intelligent Transportation Systems, 2016.