Volume 9, Issue 5, May – 2024 International Journal of Innovative Science and Research Technology
ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY2184

Blockchain-based Framework for Security and Privacy Solutions in VANET

Joseph Wheeder[1]
PG Scholar
Department of CSE, School of CSE,
Sandip University, Nashik, Maharashtra, India.

Sivaram Ponnusamy[2]
Professor
School of Computer Science and Engineering,
Sandip University, Nashik, Maharashtra, India.

Rais Abdul Hamid Khan[3]
Professor
School of Computer Science and Engineering,
Sandip University, Nashik, Maharashtra, India.

Pawan R. Ponnusamy[4]
Professor
School of Computer Science and Engineering,
Sandip University, Nashik, Maharashtra, India.

Mohammad Muqeem[5]
Professor
School of Computer Science and Engineering,
Sandip University, Nashik, Maharashtra, India.

Abstract:- The use of blockchain technology to strengthen the privacy and security of vehicle ad hoc networks has recently garnered much attention. A private and secure network for vehicular communication can be set up by taking advantage of Blockchain's decentralized and tamper-proof properties. One of the key advantages of integrating Blockchain with VANET is creating an open and immutable record of transactions. This function guarantees no one can tamper with the securely recorded data exchanges and vehicle communications. In addition, an extra layer of protection for VANET communication can be achieved by authenticating and encrypting messages using cryptographic techniques within the blockchain framework. Smart contracts, which execute themselves according to predetermined rules written into code, are another innovation that emerged from blockchain technology. VANET's security and privacy policies can be automated and enforced, making the network even more trustworthy and reliable by using this feature. By adopting a blockchain-based architecture, VANET can enhance the privacy, security, and trust between vehicles and infrastructure parts. In this paper, we look at blockchain technology, its advantages and disadvantages, and how it could solve the privacy and security issues in VANET.

Keywords:- *Confidentiality, Decentralized, Integrating, Tamper-Resistant.*

I. INTRODUCTION

Future transportation will rely heavily on vehicular ad hoc networks, which allow cars to communicate with each other and with roadside infrastructure to provide safe and practical travel. Nevertheless, several security and privacy concerns are associated with VANETs due to their open architecture. These concerns include the possibility of hostile attacks, the disclosure of sensitive information to unauthorized parties, and the necessity of building trust among network users.

Blockchain technology, initially developed to underpin cryptocurrencies, has recently attracted interest as a possible solution to these problems. Secure and private communication frameworks in VANETs can be built on top of its decentralized and immutable nature. Subsequent sections will provide a more in-depth analysis of VANET security and privacy concerns, emphasizing blockchain technology's role in addressing these issues [1]. In VANETs, vehicles share private data like their positions, speeds, and routes in uncertain and ever-changing environments. It is easy prey for cybercriminals who want to cause havoc on the network, listen in on conversations, or alter data for their ends. More than that, there are many moving parts to protecting users' privacy and the network's security [2]. three, thirty-one.

When applied to VANETs, conventional security protocols like encryption and authentication become ineffective. Their vulnerability to single points of failure stems from their reliance on centralized authorities. The security and privacy issues that must be resolved are made even worse by the absence of a solid system to build trust among the various entities in the network [3].

Blockchain technology's decentralized and unbreakable nature provides a definitive solution to the privacy and security concerns surrounding VANETs. Blockchain technology can generate an open and unchangeable record of transactions to ensure the security and veracity of data exchanges between vehicles. In

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY2184

addition, the blockchain architecture allows for strong authentication and message encryption through cryptographic techniques, which solves the problems with traditional security mechanisms [4-5].

In addition, smart contracts in blockchain technology offer a chance to automate and enforce privacy and security policies in VANET, producing an efficient and scalable way to control how nodes interact. Our goal in delving into these areas is to thoroughly understand how blockchain technology may affect privacy and security in VANETs [6].

The following sections of this article will cover the technical details of integrating Blockchain into VANETs, potential privacy and security implications, and a roadmap for future research and development on this intriguing subject.

II. MATERIALS AND METHODS

Research and interest in Vehicular Ad Hoc Networks have surged recently due to blockchain technology's potential to address privacy and security concerns. The technical complexities and practical applications of this innovative approach have been illuminated by numerous studies that have investigated the possible advantages and consequences of incorporating Blockchain into VANETs [7]. Research and interest in Vehicular Ad Hoc Networks have surged recently due to blockchain technology's potential to address privacy and security concerns. The technical complexities and practical applications of this innovative approach have been illuminated by numerous studies that have investigated the possible advantages and consequences of incorporating Blockchain into VANETs [7].

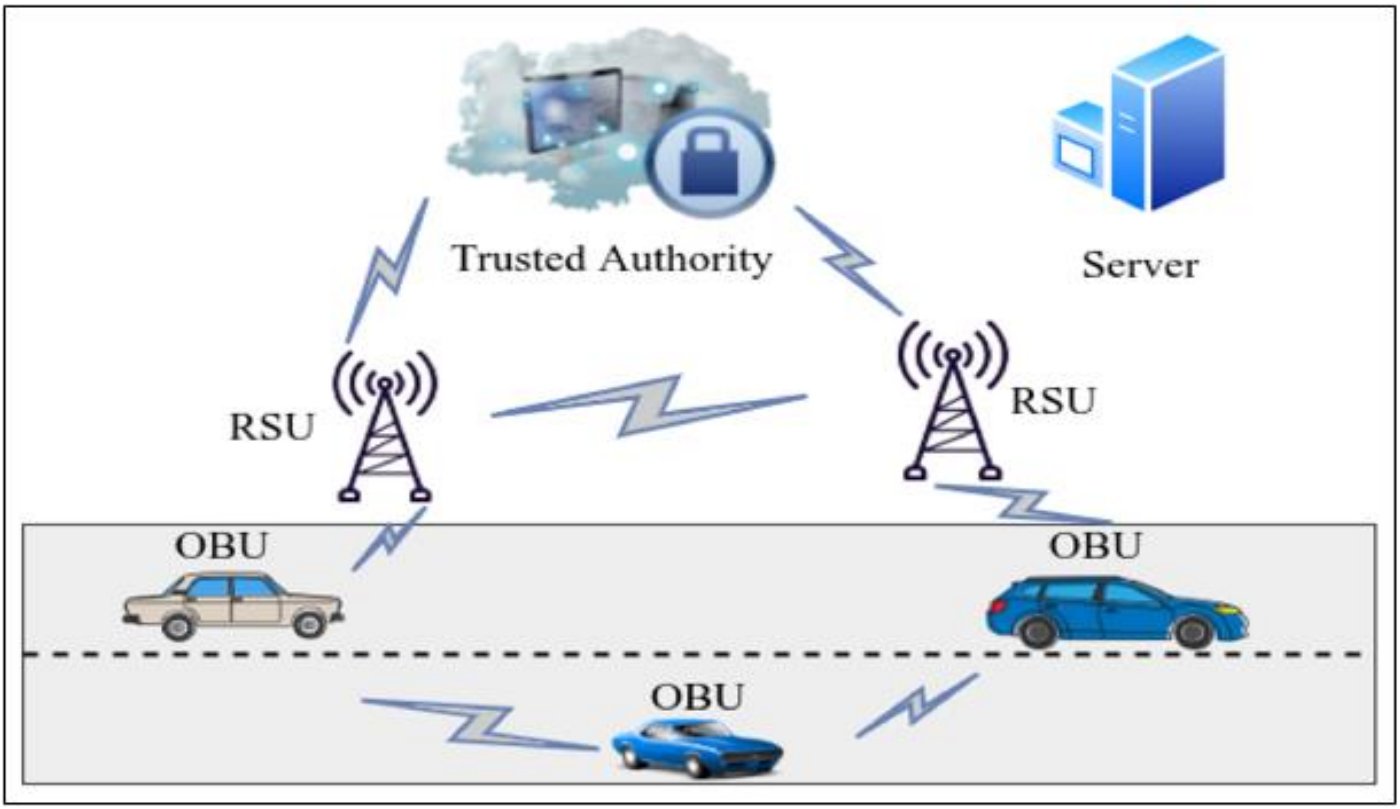

Fig 1 Explains the Architecture of VANET [29]

➢ *Technical Aspects of Blockchain Integration Into Vanets*

The architecture, consensus mechanisms, and data management strategies specific to vehicular networks, which are both dynamic and resource-constrained, have been the subject of numerous academic articles examining the technological components of incorporating Blockchain into VANETs. Innovative solutions for using Blockchain to record and manage communication transactions in a VANET environment safely have been proposed in these studies [4].

Additionally, research into improving cryptography and decentralized computing has been crucial in addressing privacy and security concerns with VANET communication through blockchain technology. Extensive research has been conducted on these technical aspects to demonstrate the feasibility and efficiency of integrating blockchain technology into VANETs, including efficient message authentication and privacy-preserving data exchange [8].

➢ *Implications for Security and Privacy in VANETs*

Studies in this field have also investigated the possible effects of integrating blockchain technology on privacy and security in VANETs, drawing attention to how it could help reduce the likelihood of attacks, guarantee the authenticity of data, and protect users' personal information. Through simulations and empirical evaluations, researchers have shown that blockchain-based frameworks are strong enough to protect sensitive information within VANETs from various security threats [9].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY2184

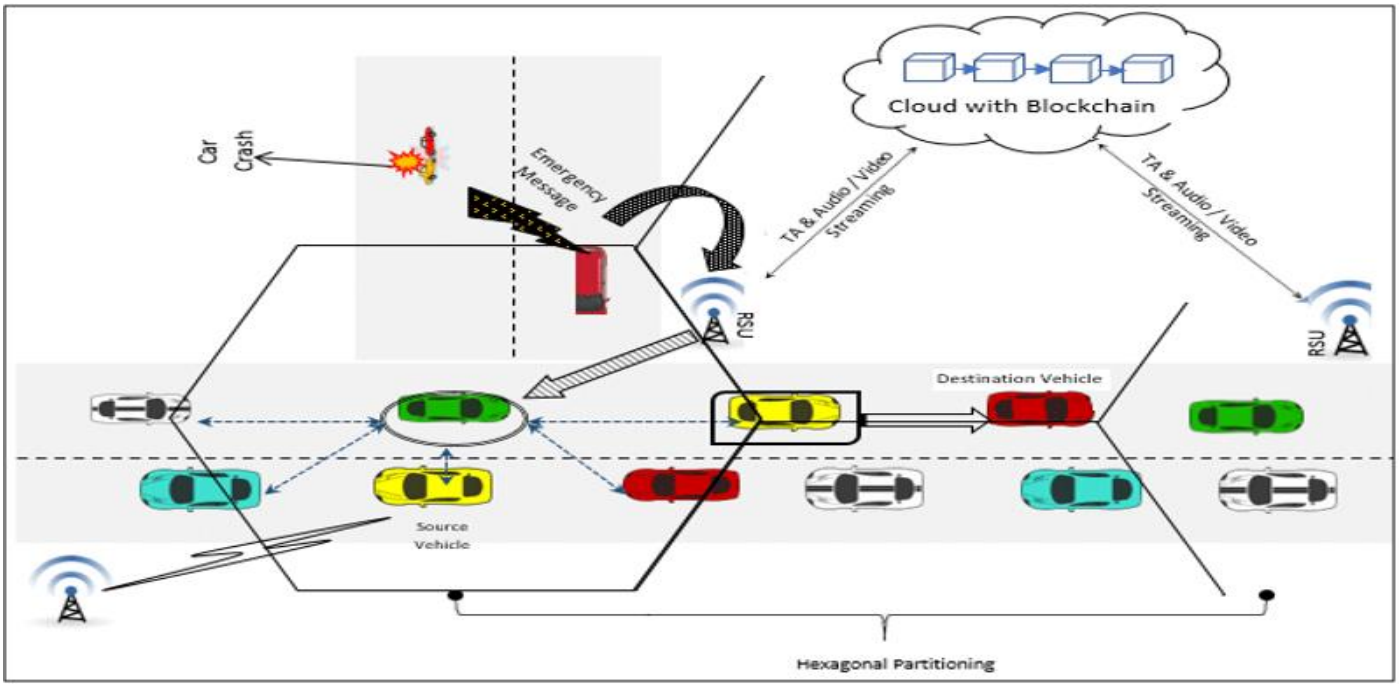

Fig 2 Explain the Implication and Importance of Blockchain in VANET [29].

Considerations like scalability, resource efficiency, and building trust among network participants are some of the economic and social aspects that have been investigated concerning using blockchain technology in VANETs. These outcomes provide helpful insight into the broader impacts of using Blockchain technology in the transportation industry, including technical, social, and economic considerations [5].

- *Proposed System Concerning VANET Blockchain Integrating*

One potential improvement to vehicular ad hoc networks (VANETs) is using blockchain technology, which could enhance privacy and security. Existing VANET privacy and security solutions suffer from problems with scalability, efficiency, and attack resistance; this system aims to solve these problems. Here are the parts that make up the proposed system:

Nodes are vehicles and roadside devices that are part of the blockchain network.

Blockchain is an immutable distributed ledger that records financial and other transactions—network security policies enforced by self-executing contracts. Our system records all VANET communications and transactions on the Blockchain, guaranteeing their secrecy and integrity. On the Blockchain, every node has its own distinct identity, and to make communications impenetrable, they are encrypted [6].

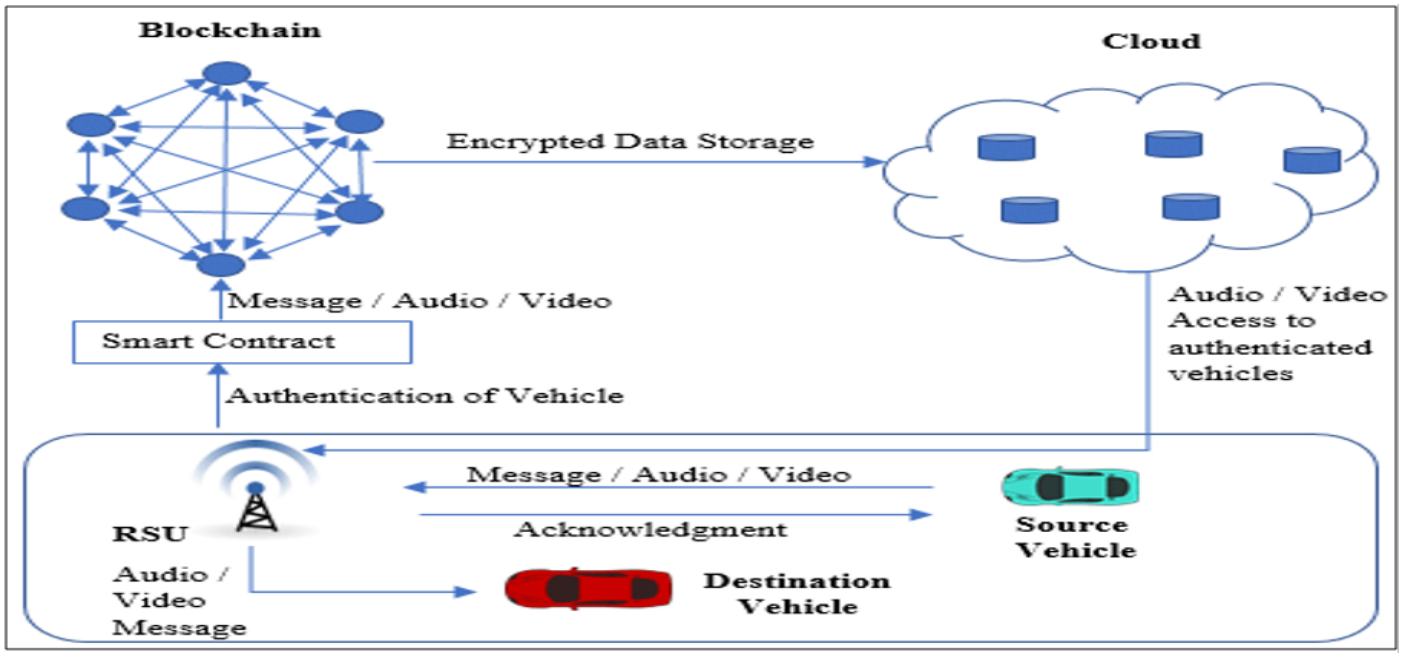

Fig 3 Explain the Blockchain Integration [29].

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY2184

This system protects the privacy of vehicle-related data through data anonymization and encryption techniques. Smart contracts are used to enforce privacy policies to ensure that only authorized parties have access to sensitive information.

The suggested system employs a consensus mechanism that works well in VANET settings, such as proof of stake or proof of authority. Limiting participation in the blockchain network to authorized nodes only protects the network from threats [12].

When considering incorporating blockchain technology into V2Ns, it's essential to build a scalable system that can handle moving vehicles' unique privacy and security issues [13].

➢ *Design Considerations for Blockchain Integration*

Network design, consensus methods, and data management strategies must be carefully considered when integrating Blockchain into VANETs. Conventional blockchain designs may be unable to handle the specific issues of VANETs in a fast-paced, resource-limited setting. As a result, the suggested system's architecture needs to consider the ever-changing characteristics of vehicular networks, such as their topology, connectivity, and data transmission rates [14].

In addition, the blockchain system's consensus mechanism is critical for keeping transaction records secure and accurate. The consensus mechanism must be strong enough to withstand assaults and flexible enough to handle vehicular communication's unique difficulties, considering the variety of network participants and the possibility of hostile behaviour [15].

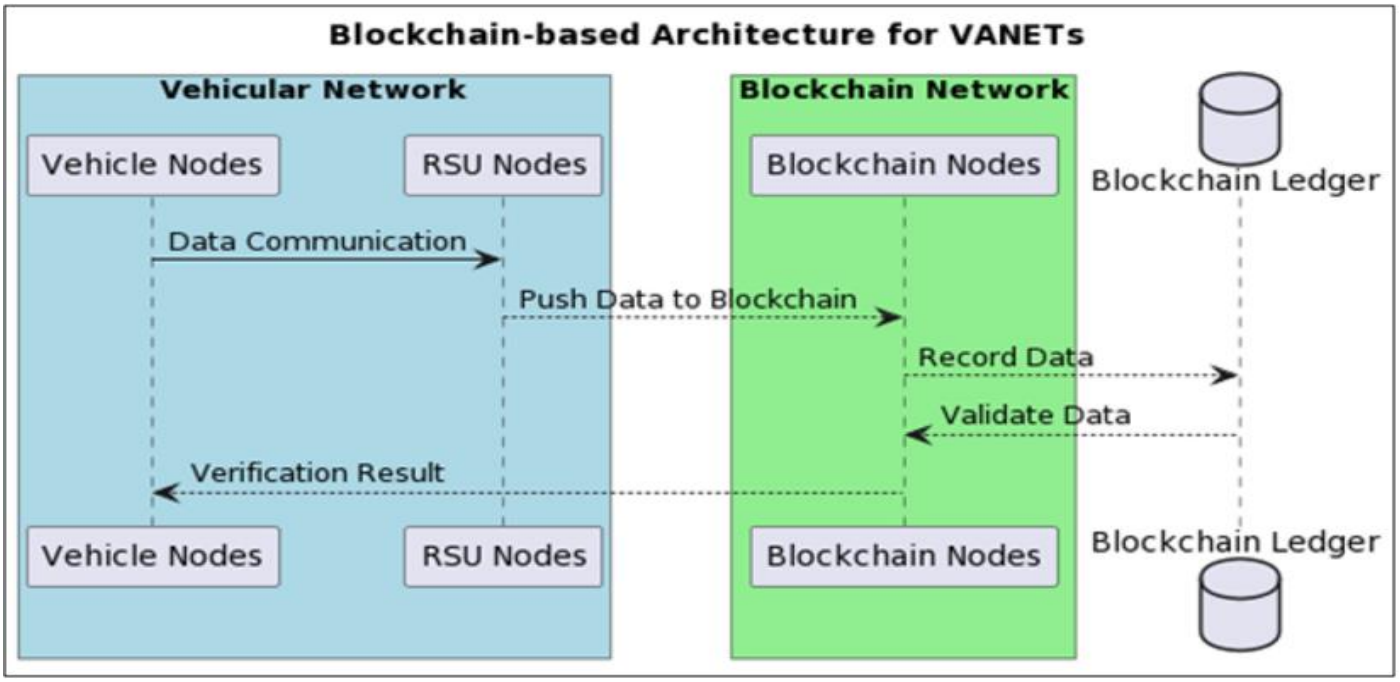

Fig 4 Competent Contact Explains [30].

➢ *Implementation Challenges and Solutions*

Several obstacles must be overcome for a blockchain-based system to work for VANETs. Particularly in a network with constrained storage and processing capacity, the overhead of blockchain transactions might be a significant obstacle. Innovative solutions like lightweight consensus algorithms and data pruning techniques tailored to the VANET context can be explored to optimize resource utilization while maintaining the Blockchain's security and reliability [16].

Furthermore, when considering integrating cryptographic methods into the blockchain framework to allow private and secure communication between vehicles, it's essential to keep key management, encryption protocols, and efficient cryptographic operations in line with the computing capabilities of the vehicles' nodes in mind.

➢ *Scalability and Interoperability Considerations*

Scalability and compatibility with current vehicular communication protocols are essential because the blockchain-based system is intended to transform privacy and security in VANETs. The system's architecture should permit smooth incorporation with preexisting VANET standards, guaranteeing compatibility and cohabitation with existing communication mechanisms while steadily improving security and privacy features [15].

Similarly, the network's efficiency and performance can't be compromised if the proposed system can't scale to handle the increasing number of linked vehicles and the volume of communication transactions.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY2184

III. RESULTS OF BLOCKCHAIN INTEGRATION IN VANETS

Blockchain technology has demonstrated encouraging results in addressing real-time vehicle network privacy and security issues. By conducting real-world simulations and empirical evaluations, researchers have proven that blockchain-based frameworks can protect sensitive information within VANETs from various security threats. The potential for blockchain integration to improve the security of vehicular communication networks is highlighted by these results [5].

In addition, the necessity for a smooth integration with current VANET standards has been highlighted in the discussion surrounding the scalability and interoperability considerations of the proposed blockchain-based system. The proposed system ensures compatibility and coexistence with legacy communication mechanisms, paving the way for a unified approach to privacy and security in vehicular environments and overcoming the limitations of traditional security measures [17][18].

These findings also affect the economic and social aspects of incorporating Blockchain into the transportation ecosystem, which goes beyond the technical domain. The research results shed light on blockchain technology's broader social and economic implications in VANETs by tackling issues like resource efficiency and trust establishment among network participants [19].

We'll review the following findings, analyzing the empirical evaluations, simulations, and practical deployment factors. By conducting this comprehensive analysis, we aim to offer detailed information about the revolutionary impact of blockchain technology on the privacy and security of VANETs.

- *Advantages of the Proposed System*

A revolutionary solution to enhance privacy and security in ever-changing automotive contexts, the suggested system for incorporating blockchain technology into VANETs boasts multiple benefits.

- *Enhanced Security and Data Integrity*

The proposed system establishes a solid basis for guaranteeing the security and integrity of data within VANETs by utilizing the distributed and unchangeable nature of Blockchain. Blockchain technology has less chance of unauthorized access because it resists manipulation. It is improving the safety of vehicle communication networks by preventing data manipulation and cyberattacks. In addition, implementing cryptographic methods within the blockchain architecture enables private and secure vehicle communication, creating a trustworthy environment for data exchange and collaboration [20].

- *Privacy Preservation and Trust Establishment*

Blockchain technology allows VANET users to maintain their privacy and build trust with one another. The proposed system creates a more trustworthy and secure vehicular communication environment, allowing for improved privacy protection for sensitive information by implementing transparent and secure transaction records. Building trust and reliability among connected vehicles is achieved through efficient cryptographic operations and fundamental management techniques, enhancing the system's privacy-preserving capabilities [21].

- *Scalability and Interoperability*

The suggested system is built with scalability and interoperability, so it can easily integrate with existing VANET standards and communication protocols. This approach makes a seamless transition and progressive improvement of privacy and safety features in vehicle environments possible, allowing blockchain-based security mechanisms to coexist with traditional communication frameworks. In addition, the system can handle the increasing number of connected vehicles and communication transactions with ease and efficiency thanks to thorough scalability evaluations [4-22].

- *Societal and Economic Implications*

The proposed system has excellent technical benefits but can also solve more significant social and economic problems in the transportation system. Integrating blockchain technology into VANETs enhances resource utilization, promotes trust establishment, and strengthens security measures. It creates an ecosystem that values data security and privacy, promotes economic efficiency, and fosters societal trust. Regarding vehicle communication networks, blockchain technology's revolutionary effects go well beyond conventional security measures and into essential areas like resource management and the development of social trust [19].

In the subsequent sections, we will further explore and elaborate on these advantages, delving into empirical evidence and real-world applications to comprehensively understand the multifaceted benefits of the proposed blockchain integration in VANETs. Through this in-depth analysis, we aim to underscore the transformative potential of this system in revolutionizing security and privacy in dynamic vehicular environments.

IV. DISCUSSION

The planned use of blockchain technology in VANETs has far-reaching consequences for social welfare in the transportation ecosystem, on top of the obvious economic and technological benefits. In the long run, people and communities benefit from the improved safety and reliability of vehicular interaction made possible by the blockchain-based system's security and privacy features [15]. Using blockchain technology in VANETs improves the security and dependability of vehicle-to-vehicle communication. Reduced congestion, fewer accidents, and improved transportation network efficiency are all possible outcomes of the proposed system's secure and tamper-proof method of sharing critical information like traffic conditions, road hazards, and emergency alerts. By reducing dangers connected with driving and encouraging a safer mobility

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY2184

environment, these improvements in safety and dependability directly influence people's health and happiness [23]. More cooperation and collaboration among network participants, including vehicle-to-infrastructure (V2I) and vehicle-to-vehicle (V2V) interactions, is made possible by the blockchain-based system's trust-establishing capabilities. The proposed system promotes traffic management, accident prevention, and overall transportation ecosystem coordination by creating a trustworthy environment through transparent and immutable transaction records. The social fabric is reinforced in this cooperative setting, which promotes shared responsibility and solidarity to guarantee safe and secure mobility and enhance the efficiency of vehicular communication [24-25]. There is potential for increasing diversity and accessibility in the transportation network by integrating blockchain technology into VANETs. The suggested system can help underserved populations, people with mobility issues, and rural areas without conventional transportation options by guaranteeing safe and dependable communication channels. A more inclusive society is promoted, and diverse demographics benefit from a more equitable and accessible transportation landscape, which is made possible through this inclusivity [15].

V. CONCLUSION

Integrating blockchain technology into VANETs in flexible transportation settings holds enormous promise for revolutionising vehicle-to-vehicle communication and enhancing societal welfare. This document's analysis has highlighted the significant implications of this integration, drawing attention to the blockchain-based system's potential for increased accessibility, inclusivity, trust, and reliability in the community and improved confidence and collaboration within it. The proposed system could be even more impactful with a few improvements and considerations. Some examples include building standards and governance frameworks for the entire industry, incorporating smart contracts, conducting data analytics while protecting user privacy, and managing trust dynamically. By exploring these future development avenues, the system can adapt to changing vehicular environments and advance societal welfare, privacy, and security. There is a greater chance for continuous improvement due to the ongoing evolution of blockchain technology and its possible synergies with vehicular communication systems. The proposed blockchain-integrated VANET system can continue its revolutionary impact, making the transportation landscape safer, more efficient, and more inclusive for everyone if we keep an eye on new tech developments and consider the future.

ACKNOWLEDGEMENT

In writing this research paper, I was fortunate to have the advice and encouragement of my advisor, Dr. Sivaram Ponnusamy. The impact of his guidance and support on my work has been tremendous. I also appreciate the chance to have grown and learned from him as a mentor.

CONFLICT OF INTEREST

Researchers have laid out a thorough plan for future work on blockchain-based secure and private methods for VANETs, considering their potential evolution. Standardization, compatibility with current VANET protocols, practical deployment issues, and investigation of new uses beyond conventional vehicle-to-vehicle communication are all part of this road map [10]. By outlining the most pressing problems and promising solutions, researchers have set the stage for further progress in this dynamic area, pointing the way toward future efforts to use Blockchain technology to strengthen the security and privacy of VANETs [6–11].

Following this introductory section, we will present our significant findings and future research recommendations after a comprehensive review of the existing literature. As a result, you'll be well-equipped to learn about the current state of the art and potential future developments in VANET security and confidentiality solutions built on the Blockchain.

Beyond the many benefits already mentioned, the planned incorporation of blockchain technology into VANETs paves the way for additional improvements and considerations that could increase the system's potential influence on the safety, privacy, and social welfare of ever-changing vehicular environments. The VANET system that uses blockchain technology has room for improvement in dynamic trust management [32]. A system's responsiveness and effectiveness could be significantly improved by adapting trust levels and parameters in real time as vehicular environments change and face different scenarios. The proposed system could dynamically adjust trust parameters based on contextual cues by incorporating machine learning algorithms and dynamic consensus mechanisms, contributing to more adaptive and resilient vehicular communication networks [8-5]. Automating and enforcing agreements in vehicular communication scenarios can be achieved by incorporating smart contracts within the blockchain framework. For VANETs, smart contracts allow for automated response to safety-critical events, scheduling of maintenance, and the allocation of resources by defining and executing predefined actions based on particular conditions. The system's social and economic implications could be advanced through this integration, which could streamline coordination efforts, optimize resource utilization, and enhance vehicular communication's overall efficiency [26].

Creating data analytics methods that protect users' privacy in blockchain-integrated VANETs is one potential area for improvement. The system has the potential to preserve individual participants' privacy while enabling the analysis of aggregate vehicular data through the use of advanced cryptographic methods and distributed computing. This feature adds to the social and economic implications of the proposed system by allowing for targeted traffic management, urban planning, and infrastructure

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY2184

optimization without jeopardizing the confidentiality of sensitive information [27].

REFERENCES

[1]. M. M. Hamdi, M. Dhafer, A. F. Mustafa, S. S. Rashid, A. J. Ahmed, and A. M. Shantaf, "Effect Sybil attack on security Authentication Service in VANET."

[2]. A. N. Patil and S. V. Mallapur, "Novel machine learning based authentication technique in VANET system for secure data transmission."

[3]. B. Guehguih and H. Lu. "Blockchain-Based Privacy-Preserving Authentication and Message Dissemination Scheme for VANET." Dec. 2019. https://doi.org/10.1145/3377458.3377466.

[4]. A. S. Khan, K. Balan, Y. Javed, S. Tarmizi and J. Abdullah. "Secure Trust-Based Blockchain Architecture to Prevent Attacks in VANET." Sensors. vol. 19. no. 22. pp. 4954-4954. Nov. 2019. https://doi.org/10.3390/s19224954.

[5]. R. Shrestha, R. Bajracharya, A. P. Shrestha and S. Y. Nam. "A new type of blockchain for secure message exchange in VANET." Digital Communications and Networks. vol. 6. no. 2. pp. 177-186. May. 2020. https://doi.org/10.1016/j.dcan.2019.04.003.

[6]. T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal and M. Guizani. "A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks." IEEE Communications Surveys and Tutorials. vol. 24. no. 2. pp. 1212-1239. Jan. 2022. https://doi.org/10.1109/comst.2022.3160925.

[7]. Y. Zhang, F. Tong, Y. Xu, J. Tao, and G. Cheng. "A Privacy-Preserving Authentication Scheme for VANETs based on Consortium Blockchain." Nov. 2020. https://doi.org/10.1109/vtc2020-fall49728.2020.9348497.

[8]. C. Dai, X. Xiao, Y. Ding, L. Xiao, Y. Tang, and S. Zhou. "Learning Based Security for VANET with Blockchain." Dec. 2018. https://doi.org/10.1109/iccs.2018.8689228.

[9]. M. Arif, W. Balzano, A. Fontanella, S. Stranieri, G. Wang and X. Xing. "Integration of 5G, VANETs and Blockchain Technology." Dec. 2020. https://doi.org/10.1109/trustcom50675.2020.00275.

[10]. A. N. Patil and S. V. Mallapur, "Novel machine learning based authentication technique in VANET system for secure data transmission."

[11]. N. Khatri, R. Shrestha and S. Y. Nam. "Security Issues with In-Vehicle Networks, and Enhanced Countermeasures Based on Blockchain." Electronics. vol. 10. no. 8. pp. 893-893. Apr. 2021. https://doi.org/10.3390/electronics10080893.

[12]. R. Tomar and Sarishma. "Maintaining Trust in VANETs using Blockchain." Ada letters. vol. 40. no. 1. pp. 91-96. Oct. 2020. https://doi.org/10.1145/3431235.3431244.

[13]. J. Gao et al.. "A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks." IEEE Internet of Things Journal. vol. 7. no. 5. pp. 4278-4291. May. 2020. https://doi.org/10.1109/jiot.2019.2956241.

[14]. B. Hildebrand et al.. "A comprehensive review on blockchains for Internet of Vehicles: Challenges and directions." Computer Science Review. vol. 48. pp. 100547-100547. May. 2023. https://doi.org/10.1016/j.cosrev.2023.100547.

[15]. S. BelMannoubi, H. Touati, M. Hadded, K. Toumi, O. Shagdar, and F. Kamoun, "A comprehensive survey on blockchain-based C-ITS applications: Classification, challenges, and open issues."

[16]. Y. Inedjaren, M. Morsey, B. Zeddini, and J. Barbot. "Blockchain-based distributed management system for trust in VANET." Vehicular Communications. vol. 30. pp. 100350-100350. Aug. 2021. https://doi.org/10.1016/j.vehcom.2021.100350.

[17]. N. Ravi and C. Kapoor. "Block Chain Techniques to Detect Attacks on VANET System: A Survey." 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM). Apr. 2021. https://doi.org/10.1109/iciem51511.2021.9445311.

[18]. W. Ahmed, D. Wu, and D. Mukathe. "Blockchain-Assisted Privacy-Preserving and Context-Aware Trust Management Framework for Secure Communications in VANETs." Sensors. vol. 23. no. 12. pp. 5766-5766. Jun. 2023. https://doi.org/10.3390/s23125766.

[19]. T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal and M. Guizani. "A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks." arXiv (Cornell University). Jan. 2022. https://doi.org/10.48550/arxiv.2201.04803.

[20]. S. More, R. Sonkamble, U. Naik, S. Phansalkar, P. S. More and B. S. Saini. "Secured Communication in Vehicular Adhoc Networks (VANETs) using Blockchain." IOP Conference Series: Materials Science and Engineering. vol. 1022. no. 1. pp. 012067-012067. Jan. 2021. https://doi.org/10.1088/1757-899x/1022/1/012067.

[21]. A. Kumar, A. S. Yadav and D. S. Kushwaha. "VChain: Efficient Blockchain based Vehicular Communication Protocol." Jan. 2020. https://doi.org/10.1109/confluence47617.2020.9057801.

[22]. V. Hassija, V. Chamola, V. Gupta, and G. S. S. Chalapathi. "A Framework for Secure Vehicular Network using Advanced Blockchain." Jun. 2020. 10.1109/iwcmc48107.2020.9148201.

[23]. C. Peng, C. Wu, L. Gao, J. Zhang, K. A. Yau, and Y. Ji, "Blockchain for Vehicular Internet of Things: Recent Advances and Open Issues."

[24]. S. Kudva, S. Badsha, S. Sengupta, H. M. La, I. Khalil and M. Atiquzzaman. "A scalable blockchain based trust management in VANET routing protocol." Journal of Parallel and Distributed Computing. vol. 152. pp. 144-156. Jun. 2021. https://doi.org/10.1016/j.jpdc.2021.02.024.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/IJISRT24MAY2184

[25]. V. S. Elagin, A. Spirkina, M. Buinevich, and A. Vladyko. "Technological Aspects of Blockchain Application for Vehicle-to-Network." Information. vol. 11. no. 10. pp. 465-465. Sep. 2020. https://doi.org/10.3390/info11100465.
[26]. A. Gkogkidis, N. Giachoudis, Γ. Σπαθούλας and I. Anagnostopoulos, "Implementing a Blockchain Infrastructure on Top of Vehicular Ad Hoc Networks."
[27]. S. Azam, M. Bibi, R. Riaz, S. S. Rizvi, and S. J. Kwon, "Collaborative Learning Based Sybil Attack Detection in Vehicular AD-HOC Networks (VANETS)."
[28]. M. A. Ahmad, "VANET Blockchain: A General Framework for Detecting Malicious Vehicles."
[29]. More, Shivaprasad & Sonkamble, Rahul et al. (2021). Secured Communication in Vehicular Adhoc Networks (VANETs) using Blockchain Secured Communication in Vehicular Adhoc Networks (VANETs) using Blockchain.
[30]. Rubén Juárez, Borja Bordel (2023). Augmenting Vehicular Ad Hoc Network Security and Efficiency with Blockchain: A Probabilistic Identification and Malicious Node Mitigation Strategy. MDPI https://doi.org/10.3390/electronics12234794.
[31]. P. Sivaram and S. Senthilkumar(2016). "An Efficient On the Run in-Vehicle Diagnostic and Remote Diagnostics Support System in VANET" ISSN 1990-9233
[32]. Ponnusamy, Sivaram & Senthilkumar, Subramaniyan. (2016). Event Notification in VANET with Traffic Congestion Detection and Congestion Avoidance. International Journal of Printing, Packaging & Allied Sciences. 4. 580-591.