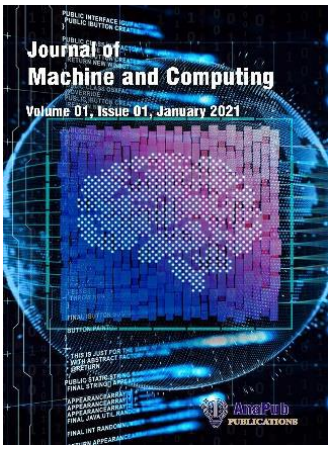
Journal Pre-proof



Decentralised Secure and Privacy Establishment in Vanet Using Key Encrypted Block Chain Scheme

Shaik Mulla Almas, Kavitha K and Kalavathi Alla

DOI: 10.53759/7669/jmc202505004

Reference: JMC202505004

Journal: Journal of Machine and Computing.

Received 18 May 2024

Revised form 22 July 2024

Accepted 22 September 2024

Please cite this article as: Shaik Mulla Almas, Kavitha K and Kalavathi Alla, “Decentralised Secure and Privacy Establishment in Vanet Using Key Encrypted Block Chain Scheme”, Journal of Machine and Computing. (2025). Doi: https:// doi.org/10.53759/7669/jmc202505004

AnaPub
PUBLICATIONS

Decentralised Secure and Privacy Establishment in Vanet Using Key Encrypted Block Chain Scheme

Shaik Mulla Almas[1*], K. Kavitha[2], Kalavathi Alla[3]

[1*]Research Scholar, Department of Computer Science and Engineering,
Annamalai University, India.
[2]Associate Professor, Department of Computer Science and Engineering,
Annamalai University, India.
[3]Professor, Department of Information Technology,
Vasireddy Venkatadri Institute of Technology, India.

[1*]mullaalmas27@gmail.com [2]kavithacseau@gmail.com [3]kalavathi_alla@yahoo.com

ABSTRACT

Using blockchain technology and smart transportation gadgets, this paper proposes the next-generation VANET system. While VANET has many advantages, it must first be improved in areas such as security and privacy if it is to be widely adopted. Nearby vehicles periodically exchange events providing their unique identifiers, locations, speeds, and statuses. Using key cryptography, it must verify the legitimacy of each car in the network before allowing it to participate, and it must take the blame for any malicious activity that occurs on the road. Due to the fast speeds of vehicles, limited communication capacity, and delay sensitive applications, traditional centralised security solutions are not applicable in VANET. The purpose of this study is to imagine a new blockchain protocol for secure event transactions in a virtual autonomous network (VANET). Blockchain is a distributed ledger system that facilitates resource tracking and administration without the need for a central authority. Therefore, a blockchain-based solution that offers transparency, tamper resistance, and immutability is preferable in a VANET scenario**.**

Keywords: Block chain, VANET, Key encryption, SHA algorithm, Consensus, Merkle tree

1. INTRODUCTION

The emergence of Vehicular smart devices is a direct result of advances in electronics and communication technology (VSD). Visionary service design (VSD) seeks to deliver insightful applications and services to enhance the security, effectiveness, and usability of the transportation network. Due to the widespread availability of smart devices, development of autonomous vehicles has accelerated. Dedicated-Short Range Communications (DSRC) modules, On-Board Units (OBUs), GPS receivers, and other sensing and localization capabilities are standard in today's vehicles. The latter facilitates interactions between motor vehicles (V2V) and other elements of their surroundings (V2I), such as other vehicles, roadside infrastructure, pedestrians, and so on. VANs, or vehicle ad hoc networks, are the result of this type of communication (VANETs). The ability of vehicles to monitor traffic conditions and relay that information to other vehicles and RSUs is a major step toward enhancing the efficiency of the transportation system. Optimized route proposals, based on factors like vehicle location and velocity, can cut down on congestion, pollution, and potential for accidents. However, certain conditions are necessary for the effective and secure operation of such programmes. The safekeeping and transmission of traffic data is of paramount importance [1]. Data integrity, data traceability, data availability, and vehicle privacy [2] are critical for constructing a trustworthy history of traffic records. Some of the current methods for protecting traffic information rely on a centralized system. The accumulated traffic data is then stored and managed in the cloud [3]. Nonetheless, such a centralized design can cause serious challenges with network congestion [4] due to privacy concerns and bandwidth constraints. Due to having a single potential weak spot, centralized designs are also easy targets for attackers.

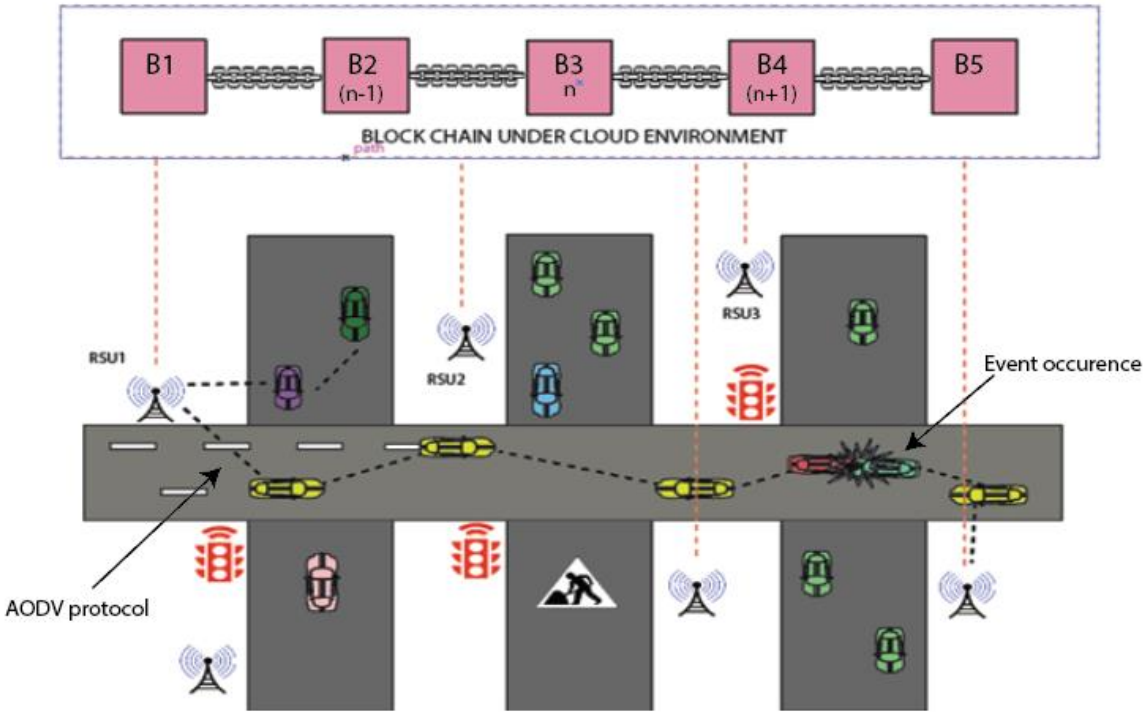


Figure 1 Block chain environment in VANETS.

2. METHODOLOGY

2.1 Model for Trust in VANETs

As shown in Fig. 2, the current trust models can be broken down into three distinct families. Trust models can be classified as either entity-based, data-centric, or hybrid [5,6]. To determine whether or not a certain vehicle can be trusted, entity-based trust models take into account the opinions of similar vehicles. Using input from neighbouring vehicular nodes, the authors provided a fuzzy method for determining a node's credibility. On the other hand, a message's veracity could not always coincide with the node's own veracity. As a result of their transient nature, vehicle nodes' trustworthiness is notoriously difficult to assess in real time [7].

Similarly, data-centric trust models [13,17] evaluate the reliability of events received from nearby cars rather than the reliability of the vehicular node itself. For their analysis, the authors of Refs. [13] turned to a Bayesian inference decision module. Since the VANET's topology is always changing, it can be challenging to collect the prior probability on which the inference module relies. Furthermore, the veracity of the message is not guaranteed by the veracity of the vehicular nodes; even reliable vehicles might be tricked into sending bogus transmissions if they are compromised. Because of this, a hybrid trust model was developed [15,19,20] that incorporates both entity-based and data-centric approaches to determining whether or not a message may be trusted. Messages from multiple vehicle nodes are used to determine the reliability of the collected data, as recommended by the authors of Ref. [20]. Additionally, functional trust and suggestion are used to assess the node's reliability. Unfortunately, data sparsity in the VANET is not taken into account by their procedures.
As a consequence of this, it is proposed that a node trust level in addition to a message trust level that satisfies all of the requirements for the hybrid trust model that will be utilised for the VNAET. Both of these trust levels will be based on the same set of criteria.

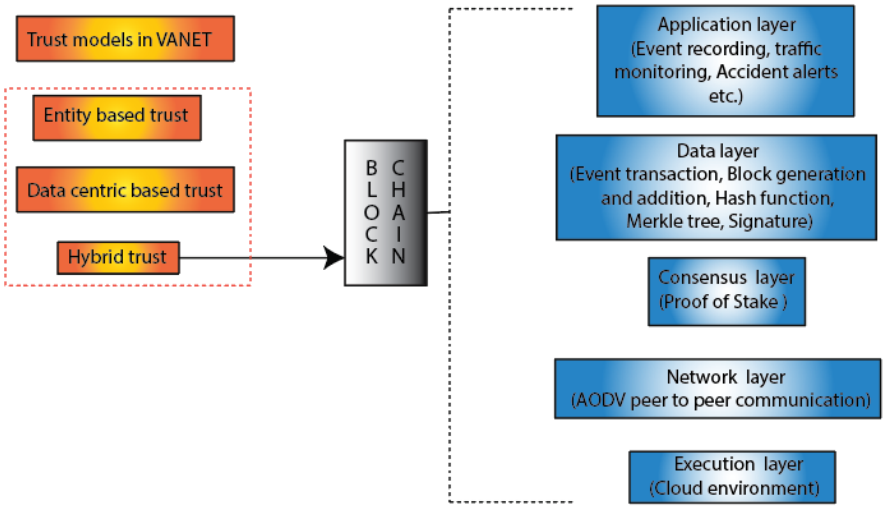


Figure 2 Trust based block chain layers for VANETS

2.2 Advantages and limitations

The following are some of the most fundamental aspects of the blockchain:

- As a result of the immutability of the data that is recorded on a blockchain, once a piece of information has been verified, it cannot be changed or tampered with in any way.
- A working environment that is not reliable due to its lack of centralization. Each node that is added to a blockchain possesses the ability to synchronize and validate all of the blockchain's contents. This enables the blockchain to function as a distributed ledger. In addition to providing security, it prevents there from being a single point of failure in the system. It instils trust where there is none to be found, which is an extremely rare occurrence..
- Users of the blockchain have greater levels of privacy than they did before it was implemented. A user is able to join the network while maintaining their anonymity. That is to say, the information pertaining to the user is shielded from view of any other users. This ensures that all sensitive personal information is kept confidential, safe, and anonymous.
- Reduced confirmation times and simplified setup mean that funds can be transferred quickly and easily. Processing a transaction or event takes only a few seconds to a few minutes, depending on its complexity.
- Because the blockchain network is decentralized, its data is reliable, accurate, consistent, timely, and generally available. It's immune to attacks and has no weak places.

3. BLOCKCHAIN SYSTEM PROPOSED

Figure 3 depicts the proposed blockchain method for secure message distribution. Every car on the network gets the latest version of the blockchain. In our approach, the blockchain records the whole history of vehicles' trust levels and event messages. When a car in the blockchain network has an event, such as an accident, it will send a message to its neighbour detailing the incident and its associated information.

It is common practice for other cars to use the LC included in an event message to determine if the sending vehicle is in the same general vicinity as themselves. The cars take into account the event notification and verify that they are in the same location. The surrounding cars then examine various aspects of the event message. Before spreading an event message farther, each vehicle individually verifies it to stop spamming, denial-of-service attacks, and other obtrusive system attacks. The mining vehicles assemble a pool of potential event messages, then examine the accepted messages for correct criteria. To determine whether or not a message may be trusted, the mining vehicle applies the following message verification policies:

• Verify the sender's reputation using the main blockchain;
• Verify the sender's reputation using the main blockchain;
• Verify the PoL using the location certificate;
• Verify that the information is first-hand;

• Verify the time-stamp

The trust level of the received event message will be increased if it is found to be legitimate and trustworthy in accordance with the verification policy. The confidence interval is calculated as the ratio of the number of verified event messages sent by vehicle V, a, to the sum of all event messages sent, a + b., i.e.,

$$TL = a/(a + b)$$

The total number of erroneous event notifications is b. Over time, the trust level shifts in response to messages that prove to be accurate or untrue. The more authentic messages a vehicle sends forth, the more reliable it is.

3.1 Assumptions

It is based on the assumption that automobiles are able to connect to the internet in an efficient manner as well as communicate with other vehicles and other objects using the V2V and V2X protocols. Additionally, it is based on the assumption that communication between automobiles and other objects is possible. All cars are assumed to include standard amenities such as OBUs, sensors, and global positioning systems (GPS). We suppose that there are more honest RSUs than dishonest ones. RSUs are typically installed as permanent fixtures beside highways. An official RSU generates a "genesis block" to kick off a blockchain based on regional happenings. Vehicles with lots of memory and a solid reputation are assumed to be full nodes that can take part in the mining procedure. Within a given geographic area, we presume that significant event alerts are transmitted within a Region of Interest (RoI). Inadequate encryption means that any adjacent car can read the crucial messages. For the sake of argument, let's say fifteen messages are needed to validate the event as true. To prevent Message Suppression/Fabrication/Alteration attacks, blockchain-based VANET represents messages sent between cars as transactions. Transactions on the blockchain need the approval of at least t RSUs to be accepted. Inter-mutual RSU consistency offers protection against transactional bias. A sequence of hash algorithms is employed to verify the chronological order and data included within blocks. The hash values of each each block are unique. The hash value of each block is brought up to date whenever the content of that block is altered. A malicious RSU that is knowledgeable about the characteristics of a hash function is able to initiate a pattern of consistent tampering if it so chooses. For example, if the blockchain's consensus is determined by the proof-of-work performed on all RSUs, then modifications to transaction information cannot be made until the percentage of invalid RSUs falls below 50%. As the chain length increased, the method's security would improve.

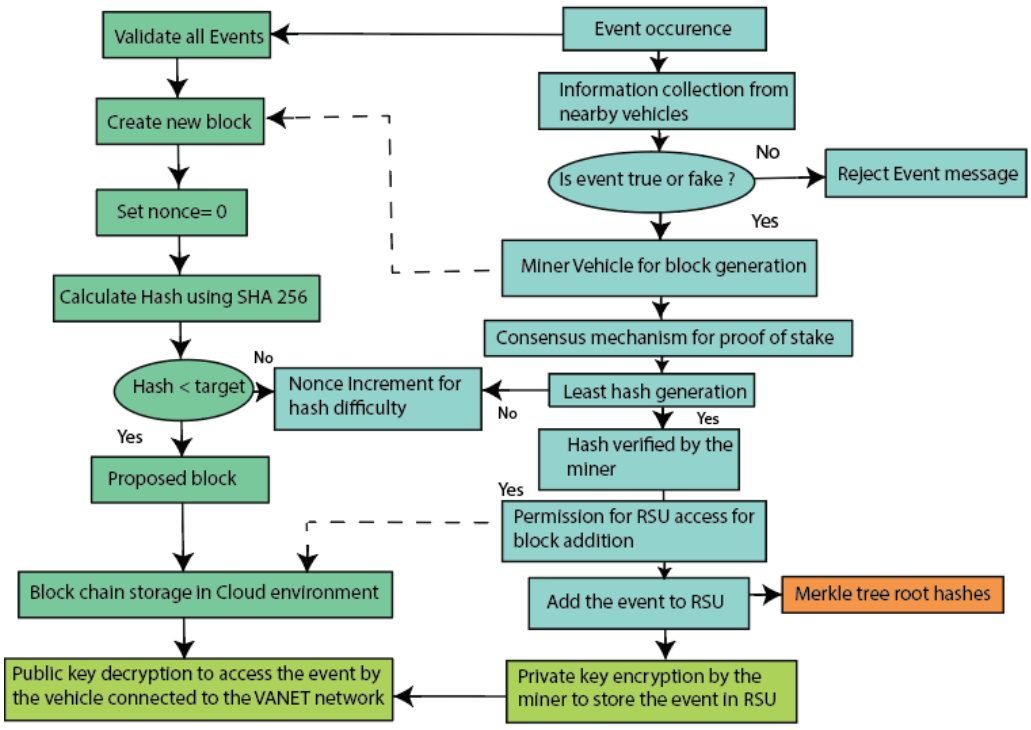


Figure 3 Proposed block chain VANET architecture

3.2 Block creation and addition

To address the problems with reliable information transfer in VANETs, a novel blockchain architecture is presented. Our method is novel because it employs the idea of a distributed public database that is immutable and accessible by all nodes in the VANET to ensure the privacy of transmitted messages. It might also be kept up by each nation on its own. This is now possible, thanks to the Bitcoin blockchain, which was developed very recently. Our issue is not the same as Bitcoin's since it involves event notifications rather than monetary transactions. For example, traffic delays, car accidents, and environmental dangers are all information that is specific to a certain area. In most cases, the information from one location or country is not particularly relevant to another. A location certificate based on Proof of Location (PoL) allows all cars to pinpoint their exact locations [17]. There are millions of automobiles worldwide; if each country operates its own blockchain, there will be less scalability concerns than with a unified network.

3.3 Block format in VANET

To address the problems with reliable information transfer in VANETs, a novel blockchain architecture is presented. Our method is novel because it employs the idea of a distributed public database that is immutable and accessible by all nodes in the VANET to ensure the privacy of transmitted messages. It might also be kept up by each nation on its own. This is now possible, thanks to the Bitcoin blockchain, which was developed very recently. Our issue is not the same as Bitcoin's since it involves event notifications rather than monetary transactions. For example, traffic delays, car accidents, and environmental dangers are all information that is specific to a certain area. In most cases, the information from one location or country is not particularly relevant to another. By utilising a location certificate that is based on Proof of Location (PoL), [17] all cars are able to know their precise locations. There are millions of automobiles worldwide; if each country operates its own blockchain, there will be less scalability concerns than with a unified network.

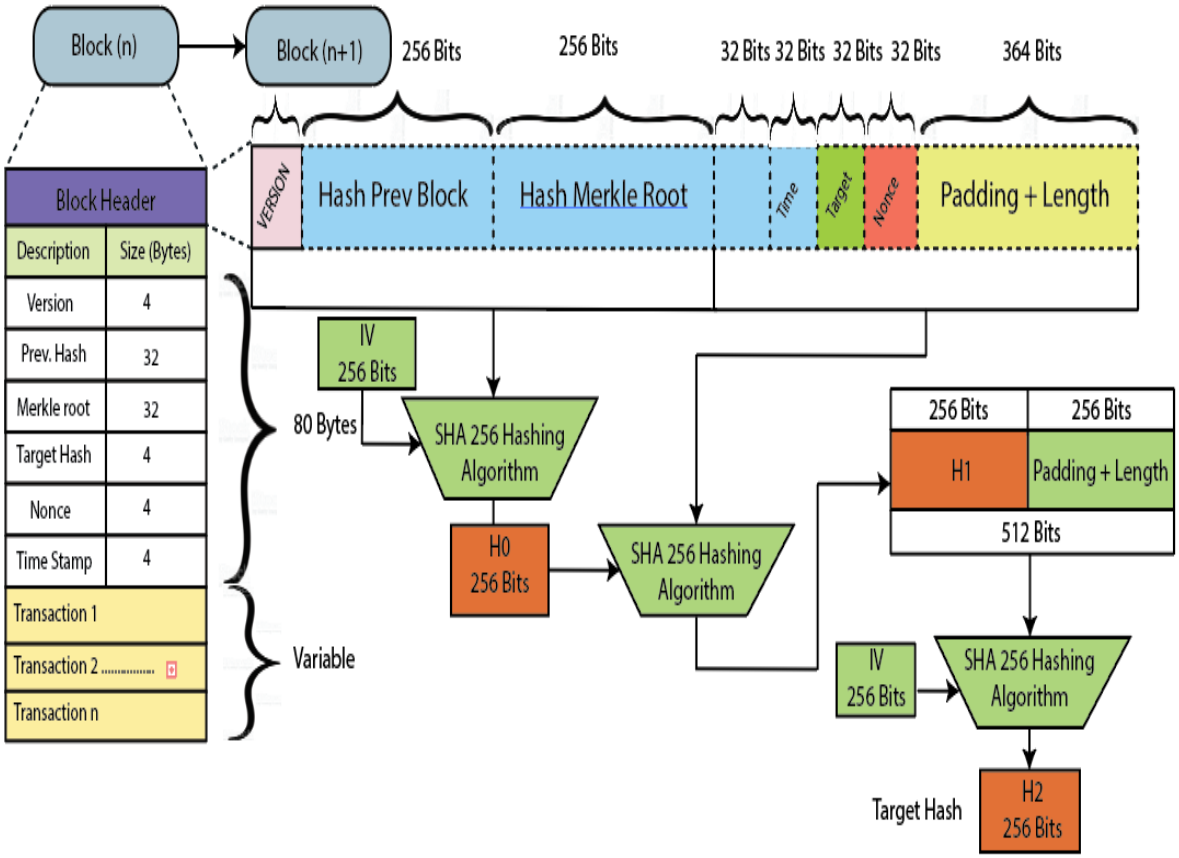


Figure 4 Block header creation & format for the suggested architecture

Mechanism for consensus (proof of stake)

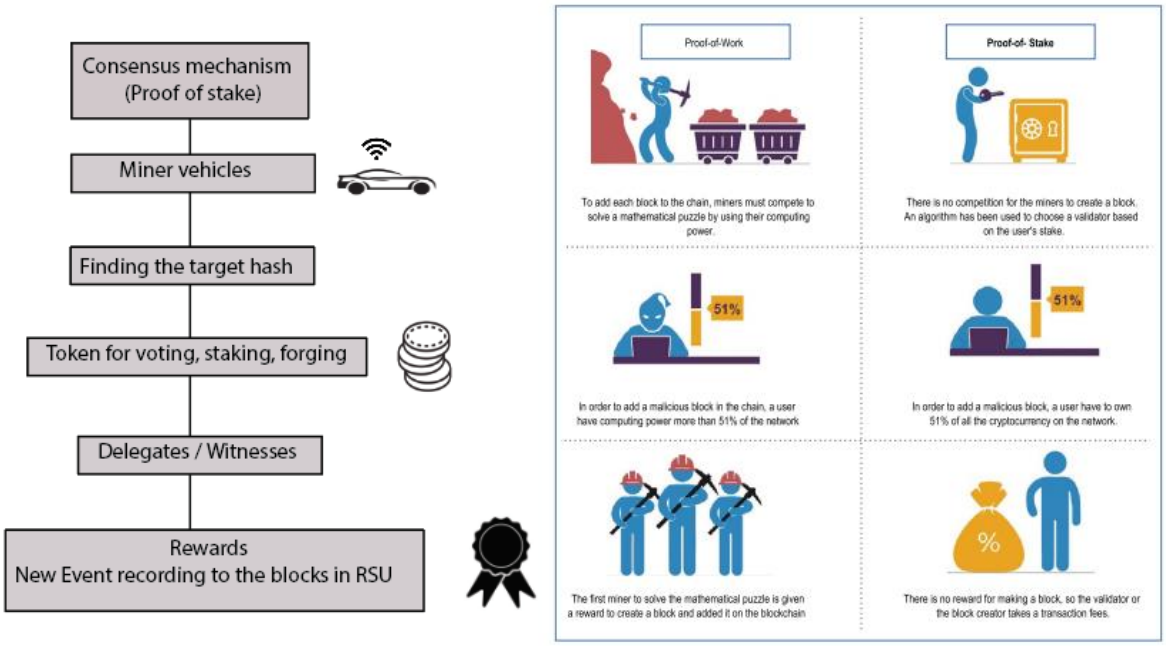


Figure 5 Schematic flow of POS consensus mechanism

Proof of Work (PoW) and Proof of Stake (PoS) are the two types of consensus algorithms that are utilised in public blockchains the most frequently. Below are the parameters for categorising consensus processes [17]. The VANET's blockchain implementation must include these methods.

3.4 Proof-of-stake (PoS) with delegation:

In this Proof-of-Stake variant, the wealthiest person selects other participants to join the network and sign blocks on his or her behalf. This means that the partner with the largest balance is able to exercise voting control over the other partners and reap the benefits of their votes. BitShare operates as a DPoS platform. The consensus process employed by the public blockchain is called proof-of-stake (PoS), and it is the one that is both the most common and the simplest. Malik et al. presented a three-tiered trust management architecture that makes use of a consortium blockchain in order to facilitate the tracking of interactions that take place within the supply chain and the dynamic assignment of trust and reputation ratings. Figure 5 is a diagram of the suggested consensus procedure.

3.5 SHA 256 algorithm

After a miner has successfully located the new block, it will be broadcast to the network along with the hash of the prior block so that it may be verified. A miner on a network is given a target, which is a 256-bit number that is completely unique to them. In order for a block's SHA-256 hash to be accepted by the network, it must have a value that is either lower than or equal to the target that is currently in effect.. The amount of leading zeros in the target determines the complexity of a cryptographic puzzle. As the objective decreases, it becomes increasingly challenging to produce a block. The difficulty of determining such a nonce will increase exponentially if leading zeros are added to the target integer. You may probably guess that judging the nonce will become increasingly challenging as the level of difficulty increases. If you increase the objective by one leading zero, you make finding the nonce 50% more difficult. The blockchain infrastructure itself determines the difficulty. The general rule of thumb is to adjust the difficulty so that it is roughly proportionate to the total network effort. The mining difficulty will increase by a factor of two if the number of miner nodes doubles. The target time for a block is maintained by occasionally adjusting the difficulty. To solve the cryptographic problem and unlock the ability to add new blocks to the blockchain, the victor must invest significant time and resources. Whether or whether such activities are rewarded is determined by the blockchain itself. Proof-of-stake consensus is a straightforward and secure method for updating and preserving the blockchain's state. It's straightforward to put into action. Every node is welcome to participate, and superior processing power may not guarantee a larger payout in this lottery-based scheme for mining. Currently, each block added to the VANET blockchain awards the winning miner with a token that may be used to add up to ten events.

3.6 Merkle tree root for event hashes

As soon as the RSU receives confirmation of an event, it enters the Transaction phase and adds the data to the blockchain. To this end, we add a Merkle Patricia Tree (MPT) structure to the proposed framework. We take inspiration from, but split the blockchain's transaction processing into two phases based on location: first, we synchronize each individual node's blockchain with the rest of the network, and only then do we attempt to bring the entire network into sync. Both the dissemination of alerts and the upkeep of the blockchain could benefit from this. Our work is organised in a hierarchical, time-based, and geographically-specific "improved MPT," a hybrid of "Merkle trees" and "Prefix trees." A leaf node on MPT is where the RSU id and the event description are both saved. Each leaf node is connected to a parent node that performs the function of an index. The root node displays the RSU allocation zone for the RSU pool. When a new block is created, it is the claimer's responsibility to communicate the details of the block to all of the RSUs that are located in the same zone. The MPT linked to the new block will store all confirmed events that occur during its lifespan. Each RSU is responsible for keeping the PoE operations of their respective blockchain zone consistent. a local-chain implementation of the union operation on MPT structures. blockchain that can only be accessed by nodes in close proximity is known as the local-chain. To unify the MPT structures of incoming events from several RSUs, local-chain synchronization is employed. Since each RSU is in possession of its own leaf node, no events will be overwritten while the RSUs synchronize. Nonetheless, the RSU confirmation of the same event will be updated to reflect the new details. You can modify the frequency with which events are recorded by changing the block's lifetime. Because it is composed of a large number of smaller chains, the global chain can split into

multiple branches. In order to find the answer, it is necessary to check the time difference. The local chain that has a first event validation time for its most recent block that is the closest to the expiration time of the block that came before it in the global chain will be declared the winner.

3.7 Block verification using RSA for RSU policy exchange

The process of verifying blocks is equally as important as producing them because it ensures that the chain's integrity is preserved. The next step is to inspect the validators' signatures that are attached to the block's hash. Since it is already known in advance in what order the RSUs' public keys will be read, only a bitmap needs to be kept. In that situation, the latter value needs to be recalculated and checked against the actual hash of the block. Each vehicle has a tamper-proof OBU key store and digitally signs and certifies periodically sent validation results.

Once an occurrence is confirmed, RSUs gather data on nearby traffic from nearby vehicles and send out alerts using DENMs. We further assume the RSU in this scenario has sufficient computational capacity to generate blocks and keep the blockchain operational over a direct cable connection. Additionally, several Certificate Authorities (CAs) issue, cancel, or cross-certify vehicle certificates. If you need quick revocation or authentication of your identity, you can look to the method. According to the findings of the LEA, the vast majority of the nodes and RSUs that make up the network are reliable participants. RSA requires two different keys—one public and one private—to function properly. It is possible to encrypt messages by utilizing the public key, which is made available to the whole public. Any message can be easily decrypted in a short amount of time if you use the private key. Both the public and private keys utilize n as their modulus, hence it is necessary to compute

$$n = ij.$$

The size of the key is measured in bits. φ Euler's totient function can be calculated as follows: φ(n) = φ(i)φ(j) = (i − 1)(j − 1) = n - (i + j -1) So long as 1 < r < φ(n), select an integer r such that gcd(e, φ(n)) = 1, indicating that r and (n) are co-prime. The exponent of the public key, r, is made available. Encryption is typically more effective with a short bit length and a low Hamming weight, such as 216 + 1 = 65,537. However, it has been demonstrated that smaller values of r (such as 3) are less safe in some contexts. x Find d by writing d ≡ r− 1 (mod φ(n)), where d is the multiplicative inverse of r (modulo φ(n)). The extended Euclidean algorithm is commonly used to calculate this. The public key is constructed using the modulus n and the public exponent r, which is also referred to as the encryption exponent. Together, these two components make up the public key. The exponent d is preserved so that it can be used as a component of the secret key. Because they play a part in determining d, the values of I j, and φ(n) must also be kept a secret.

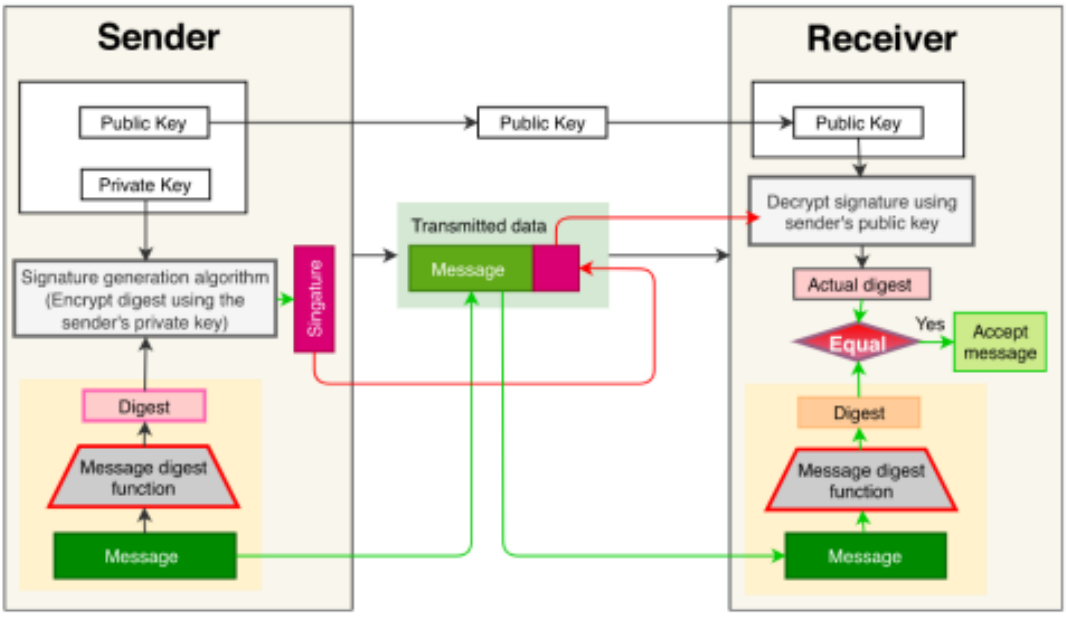


Figure 6 Merkle tree encryption key

Event type and acquisition

Table 1 Proof of Event format

Message Structure	Details
VID	Vehicle temporary ID
Event ID	Particular Event storage ID
Type of Events	Accident, Traffic, Road blocks
Time Stamp	Event recording time
Location	Local coordinates with respect to RSU
Level of Trust	m/(m+n)
Direction	Driving direction
POL	Proof of location

Many different types of traffic data are included in the ETSI-defined data dictionary for ITS applications and services. Vehicles can be used to verify whether another vehicle is travelling at the speed limit by, for instance, analysing location and speed data to detect excessive speeding or sudden stops. This can be done by monitoring the data transmitted from the car's onboard computer. However, there are some situations that are difficult to monitor through other vehicles or road amenities, particularly while the vehicle is in motion. One example of this is the human dilemma that occurs in autos when there is traffic. Further, a certain minimum number of notifications is needed to confirm an event. Here, we switch from letting other cars decide whether or not the total number of alerts is more than the threshold to having vehicles and RSUs make that call jointly.

Close by vehicle nodes will send out an event message M; whenever something happens. A vehicle can broadcast information, and its neighbors can pick it up on their own vehicles' receivers. All of the data shown in Table 1 is included in the event message. Each time an event communication is sent out over the network, every vehicle that is part of the network verifies that it is still accurate. This includes the event type, pseudo-ID, event ID, trust level, timestamp, proof-of-life, and any other relevant information. In such a scenario, the message is only removed from the memory pool of the local computer.

4. SIMULATION

Table 2 Simulation parameters

Descriptors	Range
No. of RSUs	10
Consensus group size	3-35
Events arrival rate	100-10000
Transaction size	1200 bytes
Maximum no. of transactions per block	5000
Node to node data speed	120 Mbps
Delay time	1-20 ms
Number of vehicles in network	55
Number of Miners	10

To test the efficacy of the suggested approach, we examine a number of scenarios and use a wide range of metrics. A workstation known as an HP Z230 comes preinstalled with the Windows 10 operating system, an Intel(R) i7 CPU with a clock speed of 2.80 GHz, 8 cores, and 32 gigabytes of random-access memory (RAM). We have dynamically launched a blockchain network with a range of different configurations on a single machine that shares the same features as the other systems. The MATLAB R2021 programme and built a protocol module for it. In addition, we use the MATLAB module to create the Rivest-Shamir-Adleman protocol [ref] for encrypting and decrypting messages with SHA-256. Additionally, all RSUs stay connected to one another through TCP. In addition, vehicles can transmit the gathered information via a 27 Mbps channel thanks to a WAVE (Wireless Access Vehicular Environments) module built in MATLAB using the 802.11p @ 10 MHz protocol.

To generate road traffic events is cars' primary purpose; how those vehicles go from place to place is outside the purview of this paper. Some simulation parameters are set in stone based on the metrics under study. For instance, that the maximum size of a single transaction (event message) should be 800 bytes, and that the maximum size of an individual event-transaction should be 300 bytes. A Poisson distribution is followed by the number of events that are produced by vehicles on a parameterized basis per second. If no further information is provided, the speed of the network is 100 Mbps, the latency of p2p connections is 1 millisecond, and the block timeout is 500 milliseconds (n =20; k = 10; f =2000; bs = ∞). . The configuration options for the simulator are outlined in Table 2**.**

5. RESULTS AND DISCUSSIONS

5.1 Block chain metrics

Figure 7 illustrates a clear trend of increasing throughput as both the number of vehicles and Roadside Units (RSUs) in the network expand, demonstrating the scalability and efficiency of blockchain technology in dynamic environments such as Vehicular Ad-hoc Networks (VANETs). The throughput, defined as the rate of transaction processing within the system, shows significant increases: RSU-4 configurations see a jump from 2.5 to 4.0 transactions per second as vehicles increase from 10 to 50, a 60% rise; RSU-6 configurations improve from 3.0 to 4.5 transactions per second, a 50% increase; RSU-8 configurations grow from 3.5 to 5.0 transactions per second, marking a 42.8% increase; and RSU-10 configurations see a 25% increase from 4.0 to 5.0 transactions per second. These quantitative results support Zheng et al. (2017), who argue that blockchain's decentralized nature allows for scalable and efficient transaction management, critical for networks with rapidly changing densities and topologies [21]. Furthermore, the positive correlation between increased RSU counts and throughput supports Tschorsch and Scheuermann's (2016) claim that strategic infrastructural deployments can mitigate blockchain scalability issues by supporting high transaction volumes and rapid state transitions [22]. Additionally, the data corroborate Grover et al.'s (2019) assertion on the pivotal role of strategic RSU placement and density in improving data transmission rates and reducing transaction delays in vehicular networks [23]. These findings underline the blockchain system's capability to manage larger operational loads effectively, highlighting its potential for real-world application in vehicular environments where rapid network changes are commonplace. This synthesis of empirical observations with theoretical insights emphasizes blockchain's transformative potential for enhancing data handling and security in VANETs, paving the way for more robust, transparent, and efficient transportation systems.

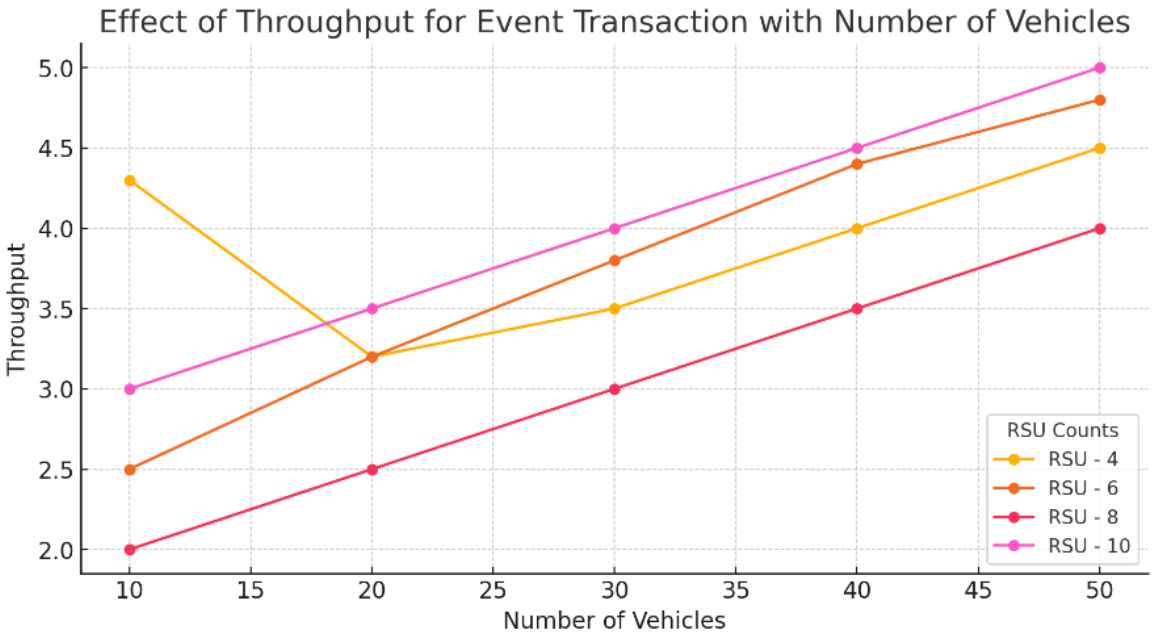


Figure 7 Effect of throughput for event transaction with number of vehicles and roadside units

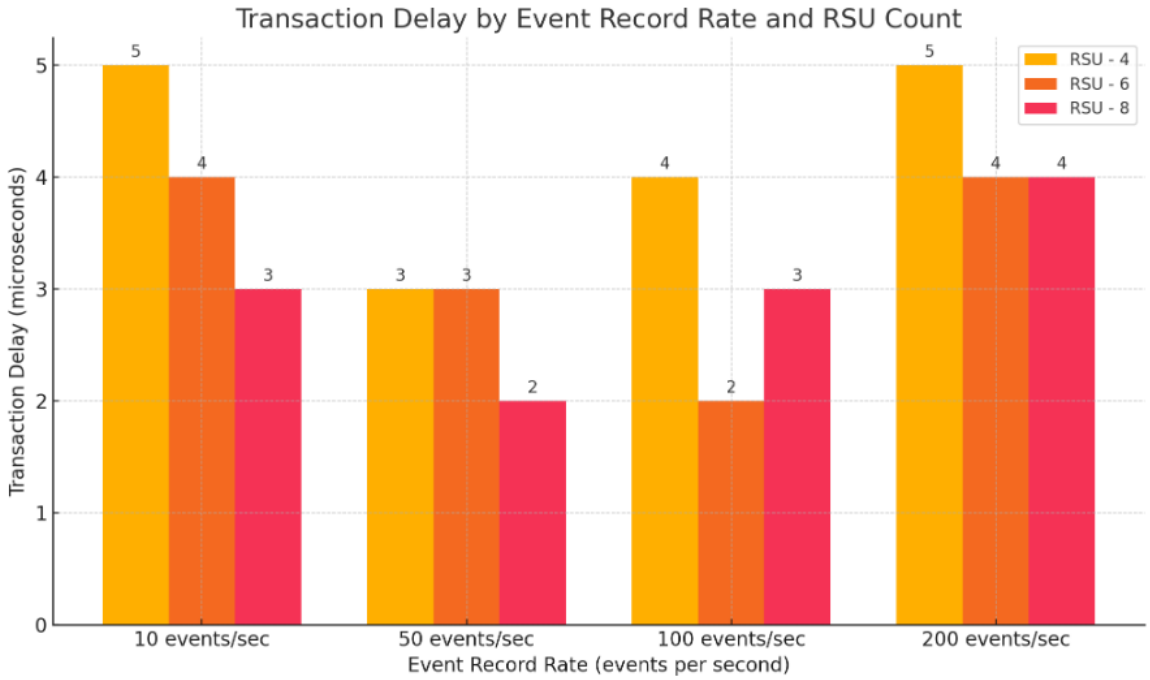


Figure 8 Transaction Delay with Event record rate for various roadside units

From RSU configurations of 4, 6, and 8, a clear observation has been made: at the lowest event rate of 10 events per second, transaction delays are highest with RSU-4 at 5 microseconds, decreasing to 3 microseconds with RSU-8. As the event rate increases to 50 and 100 events per second, this trend continues, with delays diminishing significantly—most notably at 100 events per second where both RSU-6 and RSU-8 configurations register minimal delays of 2 microseconds. However, at the highest rate of 200 events per second, the delay plateaus at 4 microseconds for the RSU-6 and RSU-8 configurations, suggesting a limit to the performance improvements attainable with increased RSU deployment at higher event rates.

This resonates with the theoretical assertions posited by Zheng et al. (2017) regarding blockchain's potential to enhance distributed network efficiency through decentralized processing, thus reducing potential congestion issues—a vital attribute for dynamically changing networks like VANETs. Furthermore, Tschorsch and Scheuermann (2016) have emphasized that blockchain networks, to handle high transaction volumes effectively, must be strategically configured to support rapid state changes, a principle demonstrated by the declining transaction delays with increased RSU counts. Additionally, Grover et al. (2019) highlight the critical role of strategic RSU placement in enhancing data transmission rates and reducing transaction delays in vehicular networks, a factor underscored by the observed improvements in transaction delays with higher RSU counts in the study.

The analyzed data substantiates the scalability and operational efficiency of blockchain in managing VANETs, illustrating that while additional RSUs generally reduce transaction delays, the benefits tend to diminish at very high event rates. These findings support the integration of blockchain technology in VANET environments, guiding future infrastructure planning and deployment strategies to optimize network performance.

In this analysis, three critical performance metrics—consensus cost time, encryption overhead, and route discovery time—within a blockchain-enabled Vehicular Ad-hoc Network (VANET) were examined. The metrics are evaluated across different Roadside Unit (RSU) configurations and varying event record rates, providing valuable insights into the scalability and efficiency of blockchain technology in dynamic network environments. Figure 8 demonstrates a non-linear increase in consensus cost time as the event record rate increases from 10 to 200 events per second for RSU configurations ranging from 4 to 8. This indicates that more complex RSU setups require higher computational resources, with RSU-8 showing the steepest rise in time costs, particularly at higher event rates. For instance, at 10 events per

second, the consensus time for RSU-4 is about 0.5 seconds, escalating to nearly 0.9 seconds for RSU-8 at 200 events per second. Such trends align with findings from Zheng et al. (2017), who highlight the augmented computational load required to process and validate transactions on a decentralized ledger, emphasizing the need for efficient consensus algorithms to enhance blockchain scalability.

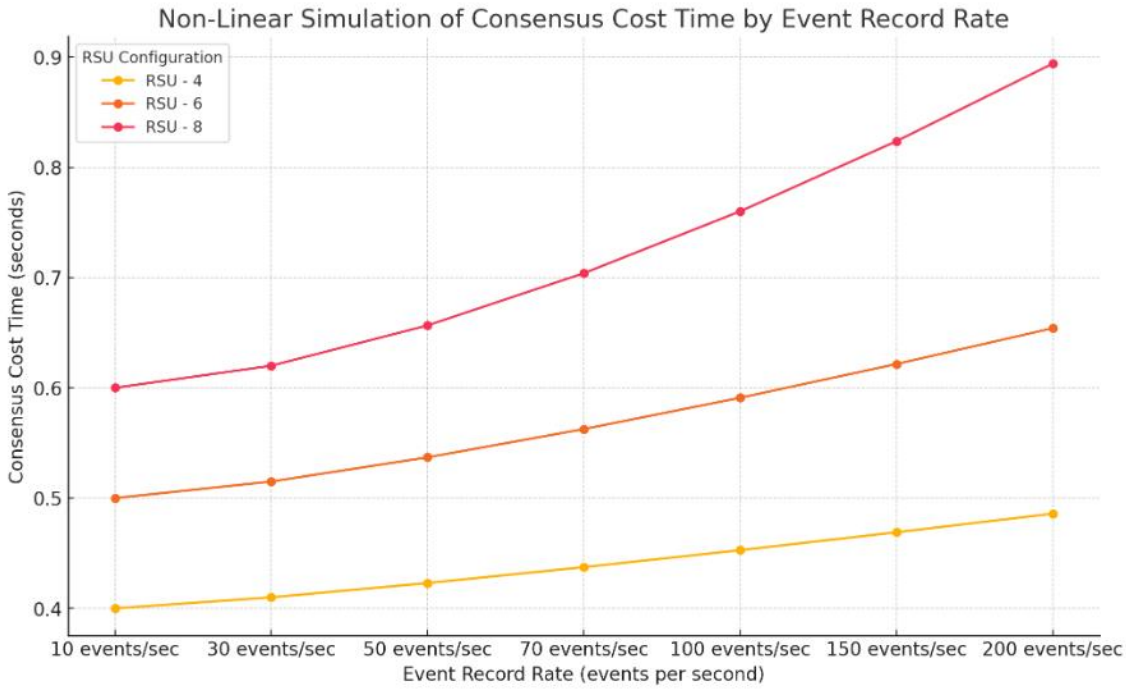


Figure 9 Transaction Delay with Event record rate for various roadside units

Figure 10 reveals a significant decrease in encryption overhead per transaction as the number of transactions increases, highlighting improvements in encryption efficiency at higher volumes [24]. For example, encryption overhead for RSU-4 dramatically reduces from 14 seconds per transaction at 700 transactions to less than 2 seconds at 900 transactions. This reduction is consistent with advancements in cryptographic techniques and hardware, as discussed by Tschorsch and Scheuermann (2016), who note the importance of cryptographic efficiency in large-scale blockchain applications.

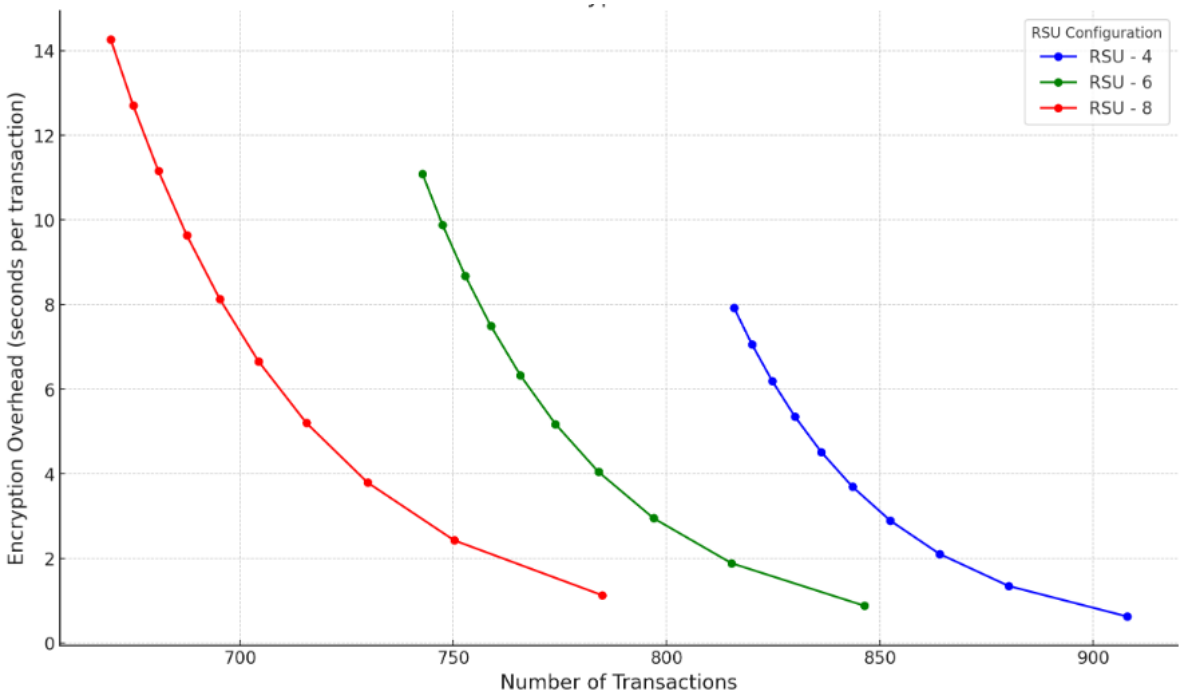


Figure 10 Transaction Delay with Event record rate for various roadside units

Figure 11 illustrates the variability in route discovery times, which inversely correlate with the event record rate. Higher event rates occasionally lead to reduced discovery times, likely due to more frequent updates that enable better synchronization among nodes. At 10 events per second, the route discovery time for RSU-4 starts at approximately 5.5 seconds, decreasing to 3.5 seconds at 30 events per second, but increasing again at 70 events per second. Grover et al. (2019) underscore the importance of efficient route discovery mechanisms in dynamic networks like VANETs, where timely data transmission is critical for safety and operational efficiency[25].

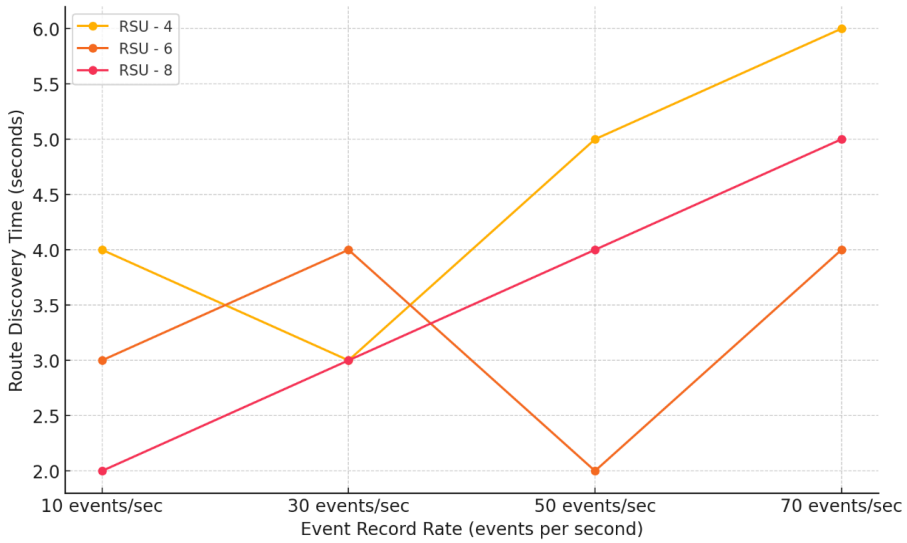


Figure 11 Transaction Delay with Event record rate for various roadside units

6. CONCLUSION

The trustworthiness of event messages can be successfully managed using our proposed method by utilizing blockchain technology. The newly designed blockchain system is capable of being run independently by its users within a single nation. This sort of blockchain remembers the

trustworthiness of both the nodes and the messages in the distributed ledger. This allows for the secure propagation of messages throughout the VANET, which acts as a source of ground truth for other vehicles. It considers event messages to be transactions rather than currencies. The The different categories of consensus mechanisms that can be utilised in blockchains are explained and investigated, and this is done on the basis of the type of blockchain. This document employs PoS consensus. All of the mining rigs for the blockchain can come to an agreement on a new block to serve as the foundation for the next block. The results of the evaluation and analysis indicate that the local blockchain solution may be utilised effectively in VANET without the need for additional storage space. This evaluation identifies a number of lingering concerns and future research domains that need be explored in order to resolve a variety of VANET security vulnerabilities prior to the technology's practical application. This is the only study that has ever attempted to analyse blockchain-based VANET security solutions in a methodical and all-encompassing manner, including a detailed review of each component. This study will encourage blockchain-based security methods in addition to boosting blockchain and VANET security.

REFERENCES

1. Xiao, S., Wang, S., Zhuang, J., Wang, T., & Liu, J. (2021). Research on a task offloading strategy for the Internet of Vehicles based on reinforcement learning. *Sensors, 21*(6058). https://doi.org/10.3390/s21186058
2. Bozorgchenani, A., Maghsudi, S., Tarchi, D., & Hossain, E. (2021). Computation offloading in heterogeneous vehicular edge networks: On-line and off-policy bandit solutions. *IEEE Transactions on Mobile Computing*.
https://doi.org/10.1109/TMC.2021.3086006
3. Cui, Y., Du, L., He, P., Wu, D., & Wang, R. (2022). Cooperative vehicles-assisted task offloading in vehicular networks. *Transactions on Emerging Telecommunications Technologies, 2022*(e4472). https://doi.org/10.1002/ett.4472
4. Jin, Z., Zhang, C., Zhao, G., Jin, Y., & Zhang, L. (2021). A context-aware task offloading scheme in collaborative vehicular edge computing systems. *KSII Transactions on Internet and Information Systems, 15*, 383–403. https://doi.org/10.3837/tiis.2021.07.020
5. Karimi, E., Chen, Y., & Akbari, B. (2022). Task offloading in vehicular edge computing networks via deep reinforcement learning. *Computer Communications, 189*, 193–204. https://doi.org/10.1016/j.comcom.2021.12.021
6. El Faouzi, N.-E., Leung, H., & Kurian, A. (2011). Data fusion in vehicular smart devices: Progress and challenges – A survey. Information Fusion, 12(1), 4–10.
7. Mecheva, T., & Kakanakov, N. (2020). Cybersecurity in vehicular smart devices. Computers, 9(4), 83.
8. Lee, E., Lee, E.-K., Gerla, M., et al. (2014). Vehicular cloud networking: Architecture and design principles. IEEE Communications Magazine, 52(2), 148–155.
9. Kaur, K., Garg, S., & Aujla, G. S., et al. (2018). Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud interplay. IEEE Communications Magazine, 56(2), 44–51.
10. Khan, W. Z., Ahmed, E., & Hakak, S., et al. (2019). Edge computing: A survey. Future Generation Computer Systems, 97, 219–235.
11. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved April 14, 2022, from https://bitcoin.org/bitcoin.pdf
12. Astarita, V., Giofre, V. P., & Mirabelli, G., et al. (2020). A review of blockchain-based systems in transportation. Information, 11(1), 21.
13. Singh, M., & Kim, S. (2017). Blockchain-based intelligent vehicle data sharing framework. arXiv preprint arXiv:1708.09721.
14. Yang, Z., Yang, K., & Lei, L., et al. (2018). Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 6(2), 1495–1505.

15. Kchaou, A., Abassi, R., & Guemara, S. (2018). Toward a distributed trust management scheme for VANET. In Proceedings of the 13th International Conference on Availability, Reliability and Security (pp. 1-6). ACM, New York, NY, USA.
16. Ding, Q., Sun, B., & Zhang, X. (2016). A traffic-light-aware routing protocol based on street connectivity for urban vehicular ad hoc networks. IEEE Communications Letters, 20, 1635–1638.
17. Al Belushi, Y. Y. O., Dennis, P. J., Deepa, S., Arulkumar, V., Kanchana, D., & Ragini, Y. P. (2024, February). A Robust Development of an Efficient Industrial Monitoring and Fault Identification Model using Internet of Things. In 2024 IEEE International Conference on Big Data & Machine Learning (ICBDML) (pp. 27-32). IEEE.
18. Wahab, O. A., Otrok, H., & Mourad, A. (2014). A Dempster–Shafer based tit-for-tat strategy to regulate the cooperation in VANET using QoS-OLSR protocol. Wireless Personal Communications, 75, 1635–1667.
19. Halabi, T., & Zulkernine, M. (2019). Trust-based cooperative game model for secure collaboration in the Internet of vehicles. In 2019 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
20. Zheng, Z., Xie, S., Dai, H.-N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14, 352–375.
21. Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18, 2084–2123.
22. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE International Congress on Big Data (BigData Congress) (pp. 557–564). IEEE.
23. Moudoud, H., Khoukhi, L., & Cherkaoui, S. (2021). Prediction and detection of FDIA and DDoS attacks in 5G enabled IoT. IEEE Network, 35, 194–201.
24. Grover, J., Gaur, M., Laxmi, V. (2016). Sybil attack in VANETs. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, 269.
25. Grover, J., Gaur, M., Prajapati, N., & Laxmi, V. (2010). RSS-based sybil attack detection in VANETs. In Proceedings of the International Conference TENCON2010 (pp. 2278-2283). IEEE.