Buletin Ilmiah Sarjana Teknik Elektro
Vol. 8, No. 2, April 2026, pp. 435-450
ISSN: 2685-9572, DOI: 10.12928/biste.v8i2.15227

Implementation of Vehicle Ad Hoc Networks for TPBFT on Latency and Fault Tolerance in Blockchain Systems

Liqaa Saadi Mezher [1,2], **Ayam Mohsen Abbass** [2], **Muna Hadi Saleh** [1]
[1] Department of Electrical Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq
[2] Department of Computer Engineering, College of Engineering, Al-Mustansiriyah University, Baghdad, Iraq

ARTICLE INFORMATION

Article History:

Received 06 November 2025
Revised 23 January 2026
Accepted 13 April 2026

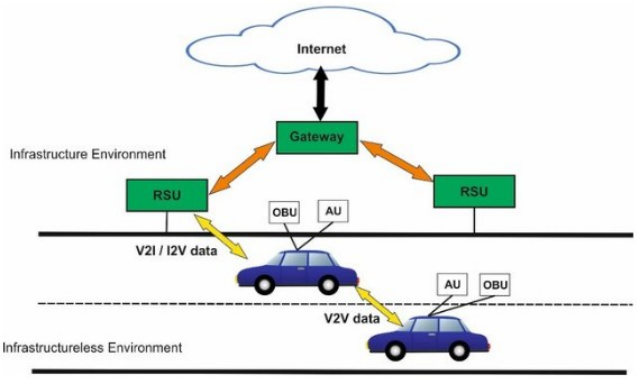
Keywords:

VANET;
TPBFT;
Latency;
Throughput;
Blockchain

Corresponding Author:

Liqaa Saadi Mezher,
Department of Computer Engineering, College of Engineering, Al-Mustansiriyah University, Baghdad, Iraq
Email:
iqa35@uomustansiriyah.edu.iq

ABSTRACT



In this paper, examines the combination of Vehicle Ad hoc Networks (VANETs) and a new consensus mechanism called Trust Practical Byzantine Fault Tolerance (TPBFT) that is aimed at improving latency and fault tolerance of decentralized vehicular networks. The VANETs are described by dynamic topology and mobile node and pose special security as well as reliability issues especially in scalable networks. The conventional Byzantine Fault Tolerance (BFT) protocols are ineffective because they incur communication overhead and scaling problems. This paper suggests TPBFT as a powerful consensus mechanism that is suitable to use in vehicular networks and is effective even when malicious or malfunctioning nodes are involved. To model real-life traffic patterns and communication scenarios, the research methodology presupposes extensive simulations based on Simulation of Urban Mobility (SUMO) tool and real-world Open Street Map (OSM) data with the help of the Python program. The performance of TPBFT is strictly tested and compared to the classic Practical Byzantine Fault Tolerance (PBFT) protocol through the analysis of the consensus latency, system throughput, and fault tolerance resilience. The findings indicate TPBFT has a shorter consensus latency (16 to 28 ms) and a greater throughput compared to PBFT and was more effective in time-constrained vehicular usage. The present work makes TPBFT an effective decentralized mechanism that allows achieving low latency, high throughput, and high resistance to Byzantine failures, offering a safe platform to deploy the blockchain technology in smart transportation systems. The optimization of the energy consumption profile of network nodes, as well as the refinement of the consensus process on the application of blockchain-based VANET architecture into practice, will be the subject of future research.

Document Citation:

L. S. Mezher, A. M. Abbas, and M. H. Saleh, "Implementation of Vehicle Ad Hoc Networks for TPBFT on Latency and Fault Tolerance in Blockchain Systems," *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 8, no. 2, pp. 435-450, 2026, DOI: 10.12928/biste.v8i2.15227.

1. INTRODUCTION

The development of the Internet of Vehicles (IoV) and the transition to the autonomous transportation system has brought a new era when vehicles are not only the means of transportation but intelligent and communicative units of a large, dynamic network [1]. These Vehicle Ad hoc Networks (VANETs) are the promise of revolution in the road safety, traffic efficiency, and in-vehicle services due to machine-to-machine real-time communication [2]. Nonetheless, the same features which make VANETs highly mobile, temporary connected, and decentralized, also make them incredibly susceptible [3]. The security, trust, and reliable data transfer in such a dynamic setting is a daunting challenge that has proven to be very difficult to overcome and which poses a risk to the safety critical base of the next-generation transportation [4].

While traditional cryptographic authentication methods offer a baseline, they often rely on centralized authorities or pre-shared infrastructures, creating single points of failure and scalability bottlenecks in widely distributed vehicular ecosystems [5]. Blockchain technology has therefore come to play as a paradigm change contender to inject decentralization, transparency, and auditability in the VANETs. The blockchain can be utilized to support trustless co-operation between the unknown vehicles by providing a tamper-proof distributed registry of events and transactions [6]. However, the integration is not that simple. It is largely because, the consensus mechanisms underlying blockchain, the fundamental protocols that make possible decentralized agreement, are designed to operate in stable and resource-rich network settings. When deployed on the volatile and delay-sensitive environment of VANETs, these mechanisms, even classical PBFT, have fatal drawbacks: too much latency, unsustainability at communication overhead, and inadequate response to realistic failure modes of intermittent connectivity and malicious node behavior [7].

This is the critical misfit in this paper. Previous studies have partially examined the performance limits of Byzantine Fault Tolerance variants in real world-constrained, large-scale vehicular simulation, actually dynamic, that can be directly compared to the real world [8]. It is not just that VANETs require a blockchain layer over the top, but that a new consensus protocol that adheres to first principle and is sensitive to vehicles network kinetics is needed. We in turn suggest and analyze TPBFT, an original consensus mechanism optimistically designed to suit the VANET context. The following are the key contributions of our work [9]-[11]:

1. A personalized consensus model: We develop TPBFT to minimize the number of consensus rounds and introduce trust metrics, thus, decreasing the latency and making the network resistant to Byzantine failures unique to vehicles.
2. High-fidelity testing model: We deploy an all-encompassing simulation system in terms of SUMO traffic simulator and OpenStreetMap which make us realistic urban mobility models which are used to test our protocol in real network conditions.
3. Strict comparative analysis: We compare TPBFT with standard PBFT in terms of performance improvements in terms of transaction latency (demonstrating a drop to 16-28 ms), system throughput and fault tolerance under the conditions of malicious actors.

The rest of this paper is organized in such a way that our work is presented systematically. Section 2 provides essential background on blockchain and consensus protocols. Section 3 details the architecture of VANETs and the specific challenges they pose. Section 4 introduces the design and mechanics of our proposed TPBFT protocol. Section 5 describes the experimental setup and simulation methodology. Section 6 presents and discusses the results of our performance evaluation. Finally, Section 7 concludes the paper and outlines directions for future research.

1.1. Background and Motivation

Vehicular networks have the potential to provide a large amount of valuable data that can facilitate the operation of many applications, such as automatic parking, collaborative intersection management, road prediction, accident reconstruction, road-space management, traffic flow prediction, cooperative lane change, automatic overtaking, and collaborative maneuvering [12][13]. The characteristics of latency, workload, determinism, limited battery, and so on need to be taken into consideration. Most important of all is understanding the reasons for supportive data sharing. The transaction details of blockchain in the operation of vehicular networks can constitute all the nodes, so using blockchain to construct a trustworthy car-assisted cooperation system has its unique advantages [14][15].

However, in the context of blockchain, practical integrity cannot be based on majority decisions since the proof-of-work's relaxed anonymity may allow the majority of attackers to be generated [16][17]. Trust Practical Byzantine Fault Tolerance (TPBFT) proves that it can quickly reach consensus among all parties (as long as there are 3f + 1 nodes in the system, where (f) is fault nodes, even with f Byzantine nodes to ensure

that they see the same control of the blockchain), but the number of communications grows in a quadratic fashion as the number of Byzantine-party nodes increases linearly [18]. We found that even in the case of electromagnetic communication, the excessive demand on the network can lead to a significant surge in faults due to various reasons [19]. The feature of synchronous group failure leads to a cold fault period in the theory of blockchain's latency, workload, and fault tolerance trade-offs among PBFT, which in turn affects the practicality of vehicular networks for many applications [20]. We must consider significant latency, throughput, and redundancy tolerance issues when improving determinism and developing a distributed-consensus blockchain for vehicular networks [21].

2. BLOCKCHAIN TECHNOLOGY

The security of the blockchain system would be impossible to comprehend without revising the technology underpinning the setup, i.e., blockchain technology. The Bitcoin cryptocurrency is the earliest and best-known application of blockchain technology [22]. At first glance, blockchain could be perceived as a distributed database. Each block is a data structure used to store transactions, and the transactions of a block are hashed. Each block's hash is stored in the next block, forming a chain known as the blockchain [23]. The blockchain is extended by creating new blocks linked to the previous blocks. In the implementation of a blockchain, two types of blockchains can be noted: public, open to any node, and private, where only approved nodes are designated to add new blocks to the blockchain [24]. No single entity controls the blockchain, as anyone within the network can utilize it, as shown in Figure 1. Since the blockchain blocks are chained and linked in a way that makes attempts at spoofing detectable, the data stored on the blockchain is immutable and regarded as non-forgeable [25].

TBFT is recognized as the consensus algorithm in the field of Trust Practical Byzantine Fault Tolerance. In fault-tolerant distributed computing, a validator group of n nodes (one-third or more of which are malicious) utilizes the TPBFT consensus model to maintain data on the blockchain network [26]. On the downside, TPBFT's competitors require a significant number of resources if they achieve a consensus mechanism on TPBFT for a large number of transactions. Commonly, validators join compared to permissionless chains, which reduces the number of validator nodes compared to permissionless chains [27].

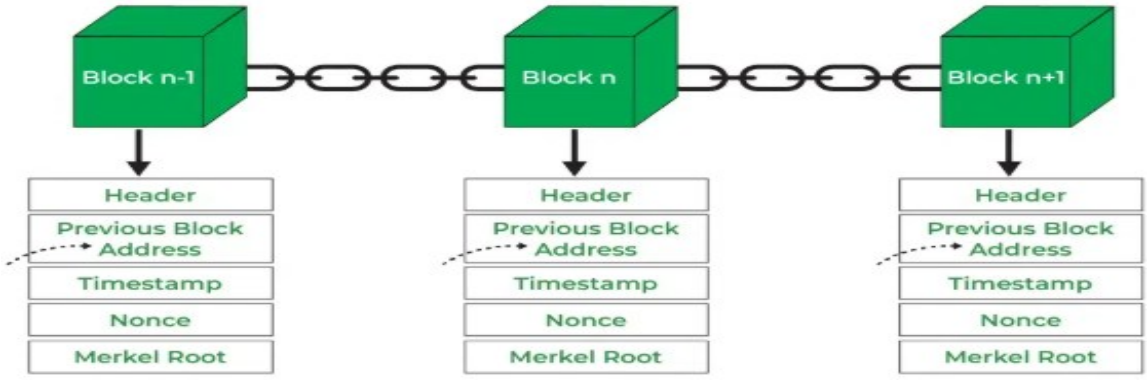


Figure 1. Structure of Blockchain

2.1. Overview of Blockchain

The traditional centralized data flow sequence is in the order of the message producer and the structure of the messages [28]. In the current age of information, providing a strictly ordered centralized sequence of responsibility is expensive and inefficient. Therefore, concerns exist about the fairness and consistency of challenges to the central authority. In order to solve this problem, blockchain provides a decentralized structure. As a result, trust mechanisms affect areas that require security, such as identity certification, centralized authorization, and information sources [29]. The significant features of centralized systems, such as the integrity, stability, and the risk protection, are also inherited in a decentralized systems [30]. However, these advantages underscore the importance of incorporating specific characteristics, notably the complexity of making changes, the inescapability of record history, and the uniqueness of individuals and logical behavior [31]. Open membership for documentation, the necessity to guarantee the protocol's efficacy, a token-creation incentives agreement, and the implementation of verification processes diminish entrance costs by increasing opposing behaviors [32].

3. CONSENSUS MECHANISMS

Consensus mechanisms play a crucial role in blockchain systems. They resolve errors and enhance reliability by achieving consensus through a distributed system [33]. One of the consensus mechanisms is the blockchain consensus mechanism. The blockchain consensus mechanism involves several parties in the system, who agree on a settlement rule and agree on the sequence of transaction processing to resolve disputes that occur in practice. In recent years, several mature blockchain consensus mechanisms have been proposed, including Proof of Work (PoW), Proof of Stake (PoS), and TPBFT [13]. Among them, PoW is the first consensus mechanism developed. It is very popular in the virtual currency market. However, PoW has the disadvantage of consuming a large amount of energy. TPBFT is a widely accepted consensus mechanism that offers low latency and high fault tolerance. It is not suitable for large-scale public blockchains. Fabric introduced the TPBFT consensus mechanism. Fabric is a practical, open-source blockchain platform and is easy to access for business applications [18].

In 2015, TPBFT appeared. TPBFT is an improved Practical Byzantine Fault Tolerance consensus mechanism (PBFT). TPBFT considers malicious behavior in cases of poor network conditions. It achieves slower internal voting in blockchain [34]. The results show that the proposed mechanism can provide better maximum TPS for different network sizes and can be used to determine the percentage of malicious nodes. In the future, the proposed TPBFT consensus mechanism can apply to private and non-private blockchains. The implementation of the VAC and TXP mechanisms is shown. Furthermore, it is also possible to compare the latency and fault tolerance between PBFT and TPBFT by constraining the consistency in both mechanisms to ensure the fastest execution speed allowed by the underlying network [35]. As an open public blockchain, the consensus mechanism must provide greater tolerance while handling a different range of transaction volumes. The goals are to implement an ad hoc vehicle network consisting of several connecting vehicles to be loaded into the PBFT and TPBFT algorithms and propose a supporting mechanism for preventing repeating taxes. That makes rare and illegal transactions useful.

3.1. Trust-Based Fault Tolerance (TBFT)

By enhancing fault-tolerant strategies, the large number of tasks on blockchain systems can be resolved. One of the fault-tolerant techniques used in blockchain systems to provide high service quality is trust-based Byzantine fault tolerance. Intelligent fault-tolerant approaches, combined with VANET use, consider latency, bandwidth, jitter, and average traffic in network layers. Considering the especially critical nature of blockchain technology in VANET, this paper focuses on the GF and TE layers. To make the comparison useful, two crucial messages regarding the validity and correctness of VANET testing are also considered as test benchmarks [36].

The transaction total execution latency periods for both PBFT and TPBFT are as follows. However, the average processing latency period for the same number of transactions for both consensus mechanisms is, and the latency for the processing blocks is. The research outcome can also assist developers in autonomous techniques for developing their systems, and the latency experiment can be further expanded to include system scalability [37]. Furthermore, the implementation of TPBFT can likely improve the traditional PBFT problems if blockchain systems are studied, given its potentially excellent results. Additionally, TPBFT has the potential to be implemented in VANET at the researchers' next stage of development [38].

4. VEHICLE AD HOC NETWORKS (VANETS)

VANETs are promising in addressing the blockchain problems of latency and fault tolerance. The ad hoc network can transmit new blocks to neighboring nodes through regular broadcasting, thereby reducing the network complexity of the entire vehicle network [39]. This study introduces a block vote algorithm, in which the leader distributes the vote information to all previously defined service nodes and allows vehicles to vote on the new block. In the TBFT, a subset of the MNs voted to decide the order of the new block in the current block generation [40]. The primary chain selection strategy of typical blockchain, proof of work, is replaced by the zero-knowledge proof in which the other participant in the V2V contact can be used to supplement the operation of packet broadcasting so that the vehicle network can still sync with new blocks and achieve the self-organizing feature of the ad hoc network in a specific time range, as shown in Figure 2 [13]. The overall BCT block voting cycle is effectively shortened, allowing it to operate as either a full node, a light node, or an SPV.

Based on the existing proven V2V intercommunication and the existing floating key to achieve trust management, the service node is designed to play an essential role in the blockchain V2X network. In this work, the BCT datagram header has been optimized for the datagram identifier and provided for the winner list of vehicles, which records the vehicles whose intersection datagrams have been received [41]. The one with the most significant number of votes is defined as the leader to construct the winner list. This study

introduces a block vote algorithm for TPBFT, and two types of service nodes are defined, which determine the state and voting role of these nodes when the vehicle becomes the new leader. Secondly, the process of vehicle transfer and the credit management mechanism for service nodes are introduced, as grouping vehicles and joining the blockchain architecture will influence the generation performance, which in turn affects the efficiency and effectiveness of BCT [42]. The blockchain-based architecture has been explained. Furthermore, it was applicable in various testing scenarios, including centralized, decentralized, and permissionless blockchains. As shown in the results section, the block interval and transmission delay exhibited a significant reduction in the system, both with and without incentives, which was faster than that of traditional blockchain systems [43].

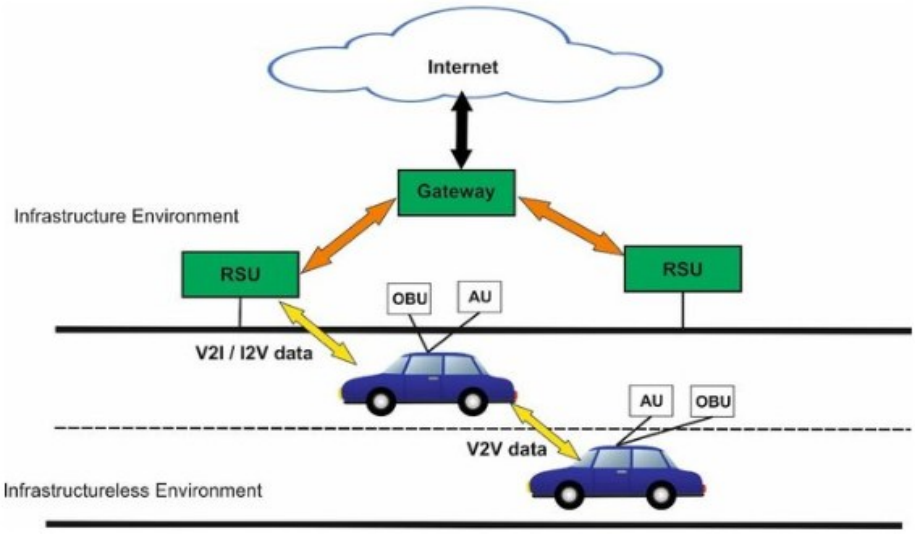


Figure 2. Architecture of VANET

4.1. Definition and Characteristics

Research into the latency and fault tolerance of blockchain, within the domain of consensus, considers the communication system in place and the transaction delay of the consensus protocol. TPBFT is unsuitable for latency in the context of consensus protocols; currently, microsecond- and millisecond-level PBFTs are a hot topic of pursuit. A thorough exploration of the consensus protocol may influence the communication system and transaction delay of PBFT. In the context of traditional PBFT systems, vehicle ad hoc networks can enhance the PBFT process [44].

The relevance of vehicle ad hoc networks prompts us to research VANETs. Our contributions are summarized as follows. The characteristics of VANETs, TPBFT, and the consensus process are illustrated. A framework for the TPBFT system of VANETs is implemented in a simulator [45]. The actual situation of VANETs is observed, and the step-by-step improvement of a consensus protocol is predicted in future work. In the research section, systems for managing director-level responsibilities are being developed, commensurate with the actual state of VANETs and node roles throughout the consensus protocol [46].

5. INTEGRATION OF BLOCKCHAIN AND VANETS

In this section, divide the existing literature into four categories according to the server that stores the blockchain: centralized, distributed, semi-distributed storage, and light nodes. Each of these has its own perspective on the VANETs and blockchain integration, and they offer different degrees of fault tolerance, efficiency, and security. From the LAN level to the VANETs, every node is connected through LAN, which forms star-type communication. The road nodes exchange messages with the main server through the base station or the access point. Once the message forwarding succeeds, the main server will send the final result to the corresponding vehicle [47].

The advantages of centralized storage are as follows: high resource utilization, easy management and operation, and low investment costs. However, the existence of the central server may cause performance bottlenecks and a single point of failure in the entire VANET system [48]. Most VANET implementations based on the blockchain adopt centralized storage. Due to the rapid growth of blockchain storage, most distributed nodes cannot host blockchain data, which can lead to serious declining performance when exploring

distributed storage, which requires homogeneous, trusted agents and a long initial sync time. However, the performance overhead may be significant. In semi-distributed storage, a small portion of full nodes is selected to store the newly generated data. This greatly reduces the storage and access cost of light nodes. A semi-distributed approach, wherein a small portion of RSU is selected as anchor nodes, allows the selected node to mine credible blocks and resolve the missing transactions in time [49].

5.1. Challenges and Opportunities

Although VANETs have some differences compared to other types of ad hoc network environments, they also share the same problems related to ad hoc communication, such as the challenges of unique identity, network connection, and reappointment of network addresses. Maintaining a unique identity, network connection, and reappointment of network addresses is only a problem during topological changes in static ad hoc network environments because the vehicle's network addresses and identities are not static and frequently change in VANETs due to high mobility [50]. Developing a VANET-unique vehicular communication environment that guarantees seamless, uninterrupted, secure communication is a bottleneck in VANET evolution and the main focus of many research topics on VANET security. Although the Certificate Authority System model briefly resolves the issues of identification and network connection in VANET, it has inevitable disadvantages when adopted in a practical VANET environment, namely a single point of failure, its cost, and other operational shortcomings. A better solution to the problems of VANET environments is to provide an authentication and agreement mechanism using blockchain [51].

However, the essential features of blockchain decentralization, fault-tolerant properties, consensus mechanisms, and decentralized power are not a good fit for energy-constrained, dynamic intermittent communication, which is characteristic of the VANET ad hoc environment. Researchers, by designing many unique applications to make VANETs more versatile, expect improvements in the V2V ad hoc environment, but implementing existing blockchain consensus mechanisms is not satisfactory for VANETs due to their associated consensus and performance problems [52]. The consensus mechanisms often consume several levels of communication messages to reach decisions in most existing blockchain systems in different VANET environments. The latency and performance issues across different consensus mechanisms can be addressed by several steps, such as optimizing the consensus thresholds depending on the emergency level, reducing communication protocols between the blockchain and drivers, switching between different consensus mechanisms in the blockchain based on vehicle density, or using a prediction-based consensus model [53]. Again, each of these newly developed solutions must choose several consensus mechanisms and their trade-offs based on the type of public blockchain [54].

6. EXPERIMENTAL SETUP

The VANETs are implemented using a SUMO simulator tool, and the mobility model is obtained from Open Street Map (OSM) traffic simulator with a protocol for V2I communication, as shown in Figure 3. The continuous network architecture protocol is used as a network enhancement for vehicle networks. The blockchain system is implemented using a distributed open-source framework.

Figure 3: OSM Web Wizard

6.1. Simulation Tools and Environments

In this section, the simulation tools and environments employed are presented. The SUMO simulator is utilized to simulate connected vehicle environments and cover a variety of parameters and features, as shown in Figure 4. We have chosen to use the Python-based network simulator to perform simulations. It is a simulator for students and researchers in the field of vehicular communication networks, enabling them to implement their own settings and environmental conditions. The paper is a source code that is based on Python, and it provides guidelines for other researchers to modify or create new scenarios. It is composed of a large set of elements that comprise the simulator, such as Mobility Trace, Field, Vehicle, and Applications.

The core simulator allows researchers to model, simulate, analyze, design, and prototype vehicular ad-hoc networks environments with a high degree of customizability and performance constraints. The simulator is designed to be open, to be used with standard programming tools, and to facilitate reusability. The simulator is highly significant, used by students and researchers to model, prototype, simulate, and provide a reference implementation to analyze and to provide guidelines on how to create new environments. In addition, the simulator can test research initiatives before actual deployment. The simulation platform's dominant performance involves gathering critical performance metrics and profiling algorithms to determine their suitability for specific requirements.

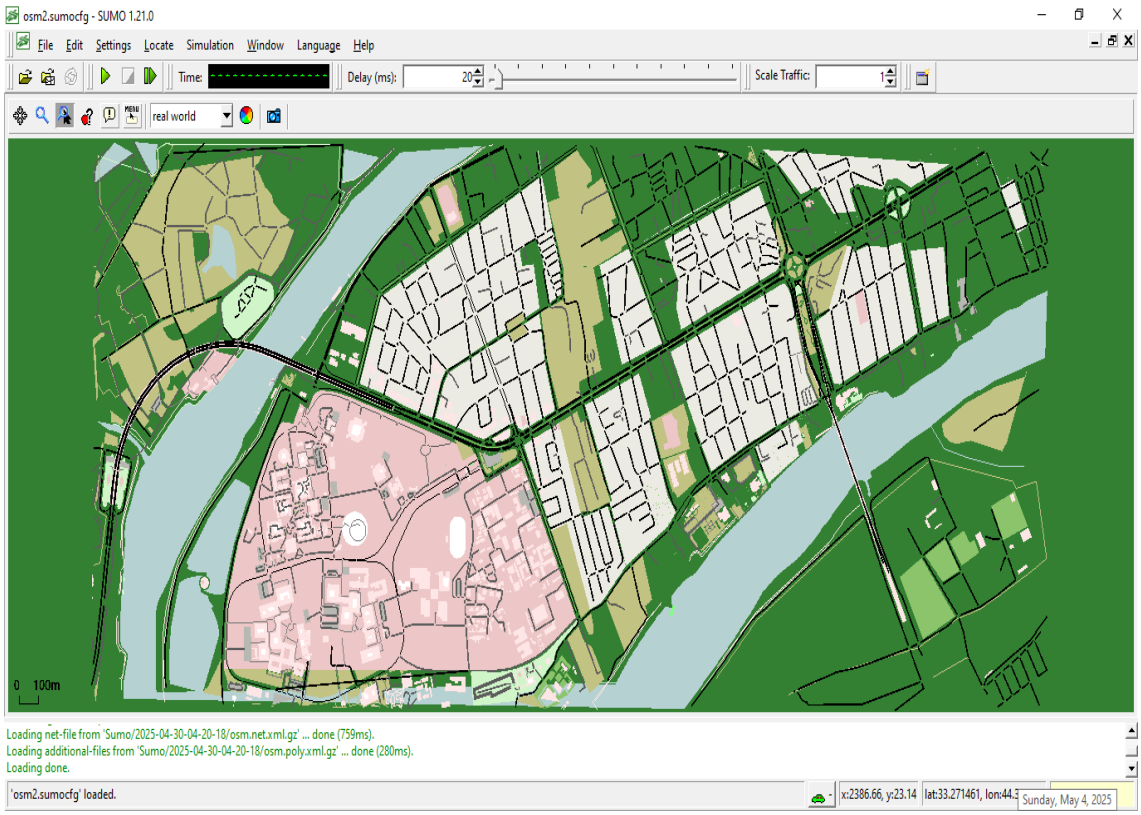


Figure 4. Data Extraction in SUMO of Area (100*100) km²

7. PERFORMANCE METRICS

Performance metrics play a crucial role in blockchain for its efficient working across the network and the applications. The major metrics that determine the performance of the blockchain system are the number of consensuses reached, the number of blocks generated, the transactions occurring across the network, and the maximum latency of the network for reaching the consensus decision. The more consensus and blocks handled, the faster the blockchain system works in terms of providing the transactions. Reduction in consensus and block generation, with increased throughput and decreased latency, has been significantly contributed to by the literature. These performance metrics can be defined as: The number of consensuses reached Number of blocks generated the overall number of transactions occurring across the network The maximum latency of the network in reaching the consensus decision, as shown in Figure 5.

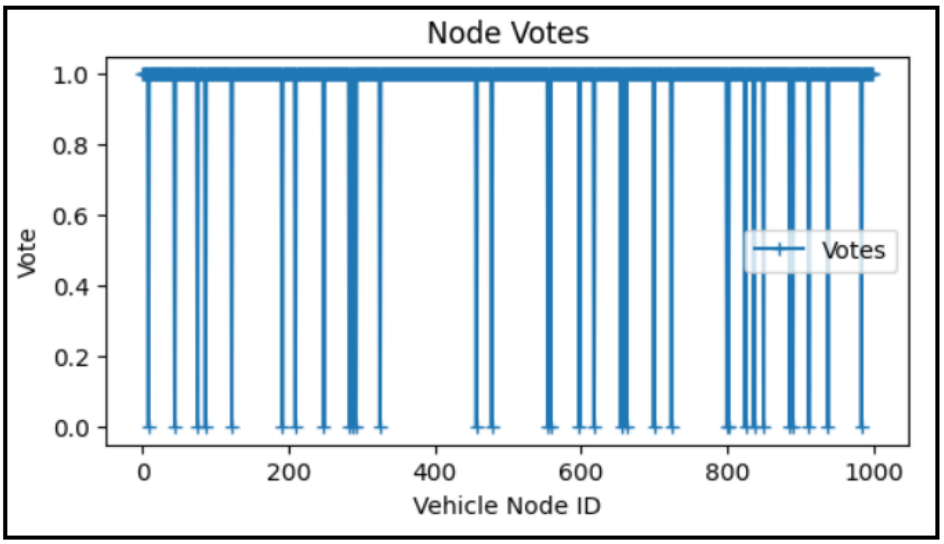


Figure 5. Consensus TPBFT of 1000 Vehicle Nodes

7.1. Latency Measurement

Latency and throughput are the main performance parameters for VANET applications. Therefore, the main goal of this study was to find the latency associated with each of the consensus mechanisms when BAS was applied as the blockchain system. The results of this study are discussed in the following section. The latency measurement of the systems is described in this section. The implementation and result analysis of both protocols are discussed in the next section as well. Latency measurement is an important aspect to consider at all levels of implementation. Every slight difference in the response time can cause a delay in this kind of communication, and for any vehicle network including critical data, that could be very crucial. It is not necessary for ships, trains, or other VANETs, but for the intelligent driving of the vehicle, latency must be less, and the correct information must be received by all connected vehicles over various distances. All of the consensus times for latency on each protocol are used, with time to block generation, then capturing the receiving time of the ledger, and a combined time difference measure for a single block of the whole number. Different data are used to compare the different consensus protocols, as well as provide different fault tolerance and throughput measurements, as shown in Figure 6.

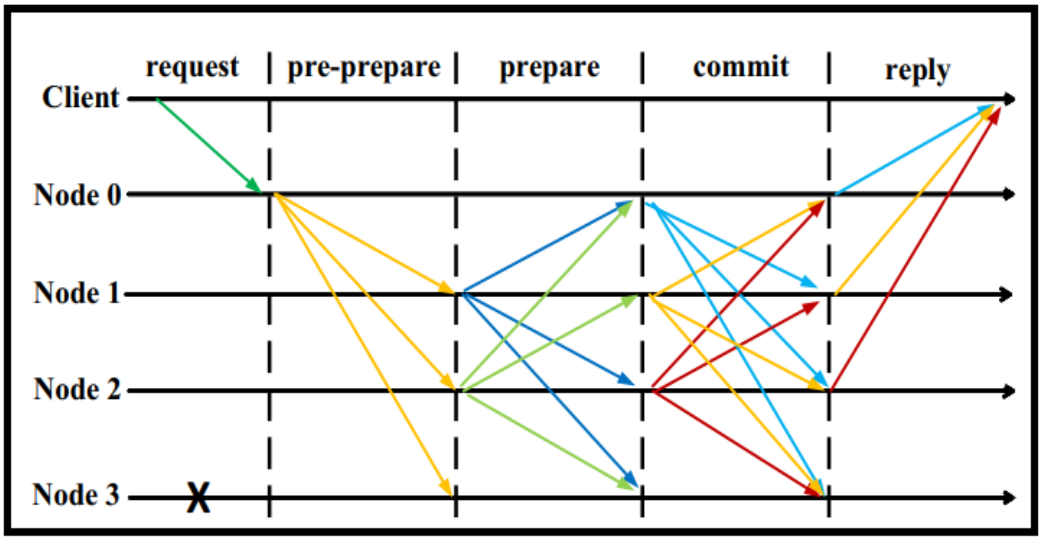


Figure 6. TPBFT Consensus Process

7.2. Fault Tolerance Analysis

Autonomous vehicles are expected to form a network to share information about the external environment in real time. A network of autonomous vehicles is a VANET, which is a temporal network with restricted

mobility, where the vehicles gather during the journey. Various efforts have been made to address this challenge based on the distributed autonomous vehicle network. In the case of actual applied systems, a consensus algorithm is required that is tolerant to mobile network faults. This text combines the V2I communications technology, which has been actively studied as a communication method for autonomous vehicles, and the blockchain-based consensus algorithm that does not depend on the frequency or quality of communication with the vehicle, and it presents and compares the results of evaluations of real-time performance and fault tolerance.

The text combines the autonomous vehicle communication method, where quality is not guaranteed and the frequency of communication is limited, with the autonomous vehicle consensus algorithm, targeting both blockchain projects and many ongoing projects for autonomous vehicles. We present autonomous vehicle models that cover the common TPBFT consensus algorithm. When combined with VANET, the typical autonomous vehicle experience blockchain disadvantages, such as latency and lack of fault tolerance, provide significant efficiency performance and more reliability in terms of disaster prevention. The advantages of the two combined systems are compared and limit latency to blockchain transactions while maintaining fault tolerance.

8. RESULTS AND ANALYSIS

This study analyzed the performance of VANET, which uses the transaction division hierarchical ECDS blockless algorithm, and compared the performance of TPBFT consensus algorithms in this context. In addition, a comparison with other systems of blockchain in VANET was also carried out. Our analysis showed that one algorithm achieves less latency than another as the number of companies increases or decreases. Conversely, the latency of the alternative algorithm tends to increase with the number of transactions. For the TPBFT algorithm performed over VANET, satisfactory fault tolerance results were presented, as long as the established computational power for each company is respected. Finally, the division of the transaction key block type used in this study to decide which company retains the committed transaction is a good choice since it presents the best results when compared to the division into sub-blocks and the verification of dependencies on the blockchain. The average latency of the transaction approval methods in the VANET achieved 28 and 16 milliseconds, respectively, of correct vehicle nodes, as shown in Figure 7.

Figure 8 represents the average latency of TPBFT phases in VANET, which contains 333 faulty vehicle nodes from 1000 vehicle nodes. The graph compares how latency varies during each phase with fluctuating numbers of correct nodes, illustrating that latency values generally range between 0.0032 and 0.0064 seconds. The network delay varied according to the structure of the network; the delay in approving transactions was directly influenced by the number of nodes in the transportation network. With the quantification of computing blocks per network context in VANETs, this study collates barriers that were focused only on hardware applications used for attack mitigation in the VANET, ensuring the trust of the blockchain.

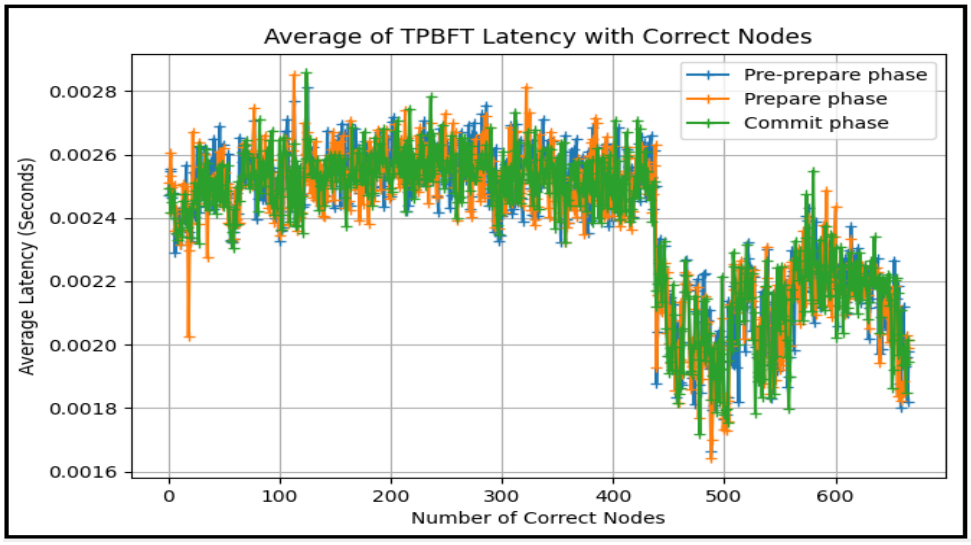


Figure 7. Average Latency of 667 Correct Vehicle Nodes of All TPBFT Phases

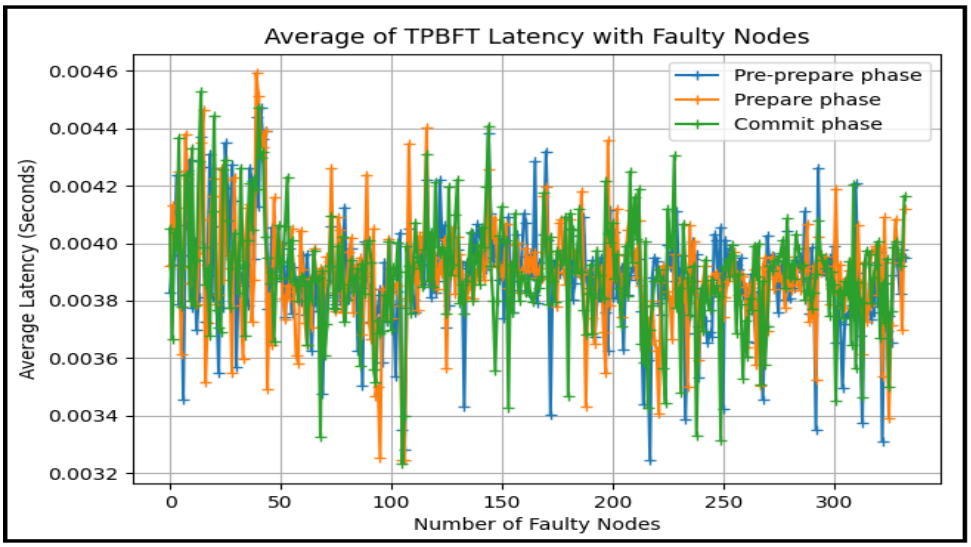


Figure 8. Average Latency of 333 Faulty Vehicle Nodes of All TPBFT Phases

8.1. Impact of TPBFT on Latency

In the following graphs, we summarize the effect of adopting TPBFT on the latency. To get a visualized and rough understanding of the performance gap, we present the data of an empty blockchain in our graphs. To have an in-depth investigation of the LTP between different blockchains under different settings, we randomly take 1000 generated nodes from the two selected blockchains and compute the median; the median is the point in the distribution of the blocks. The parent of a randomly generated block and its presentation time will effectively decrease the computational cost. Also, the bottleneck is how to get the mean and variance of the block interval and sustain the high performance of the realization. Figure 9 represents the average throughput of TPBFT phases in VANET, which contains 667 correct vehicle nodes from 1000 vehicle nodes. The graph compares how throughput varies during each phase with fluctuating numbers of correct nodes, illustrating that throughput values generally range between 0.8 and 1.4 seconds, with some spikes and dips throughout.

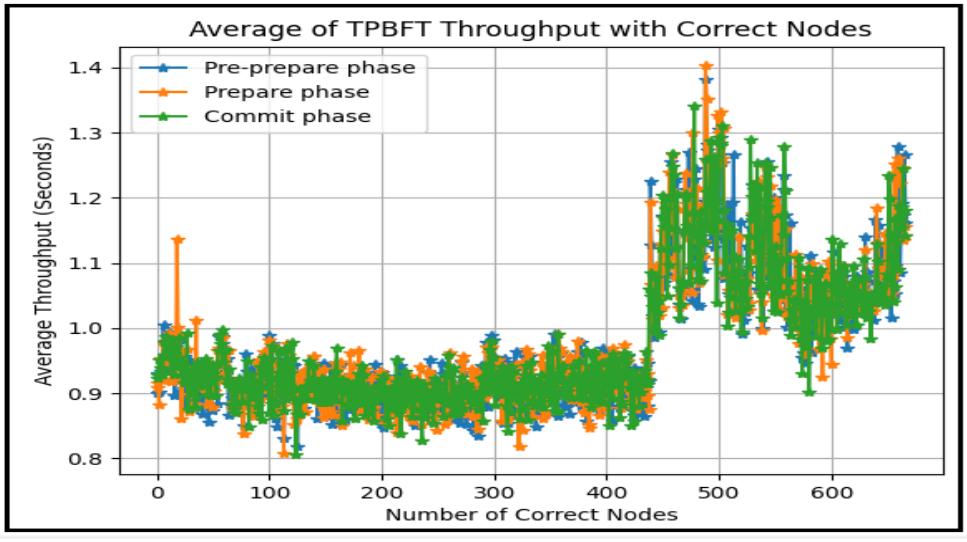


Figure 9. Average Throughput of 667 Correct Vehicle Nodes of All TPBFT Phases

Figure 10 represents the average latency of TPBFT phases in VANET, which contains 333 faulty vehicle nodes from 1000 vehicle nodes. The graph compares how latency varies during each phase with fluctuating numbers of correct nodes, illustrating that latency values generally range between 0.0032 and 0.0064 seconds. As the number of rounds in the consensus state diagram is 3 and the time spent measured by the real transaction

is far from being 0, we only include priority of error (Pe) as shown in Figure 11 and priority of censuses (Pc) in this diagram. It is observed that the VANET network has a Pe, which is a priority of error, of less than multiple seconds; however, it should be noted that some outliers even have a transaction time much greater than one minute. Since Litecoin has a large block size, the rate of a new block is very good; the rate is only lower in an interval from 6.5 to 10 minutes. For the two blockchains, TPBFT leads to a significant increase in the block rate. From the perspective of latency, the distribution time in adopting the same consensus mechanism will improve if the number of rounds is smaller, and the time to finish consensus will also decrease. The big O time of TPBFT depends on the number of rounds, representatives, and other settings.

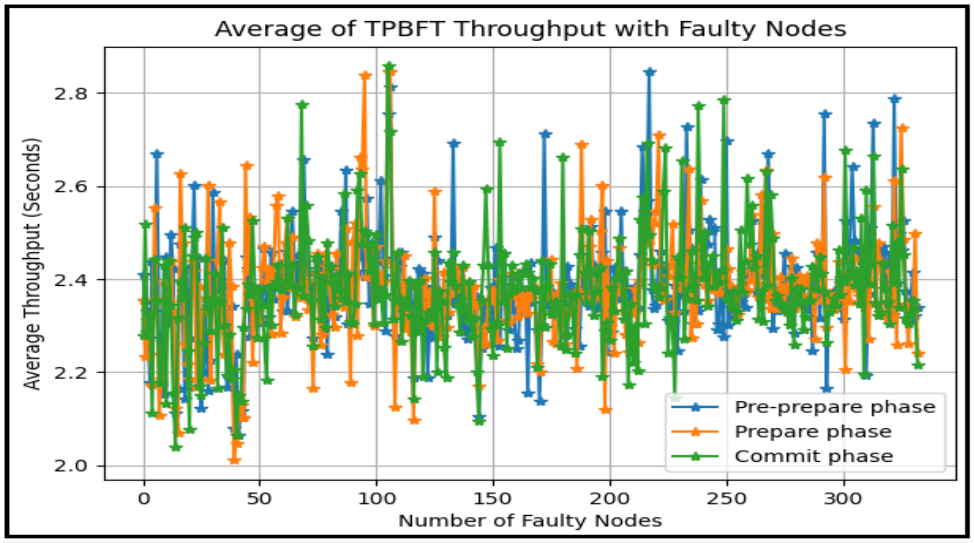


Figure 10. Average Throughput of 333 Faulty Vehicle Nodes of All TPBFT Phases

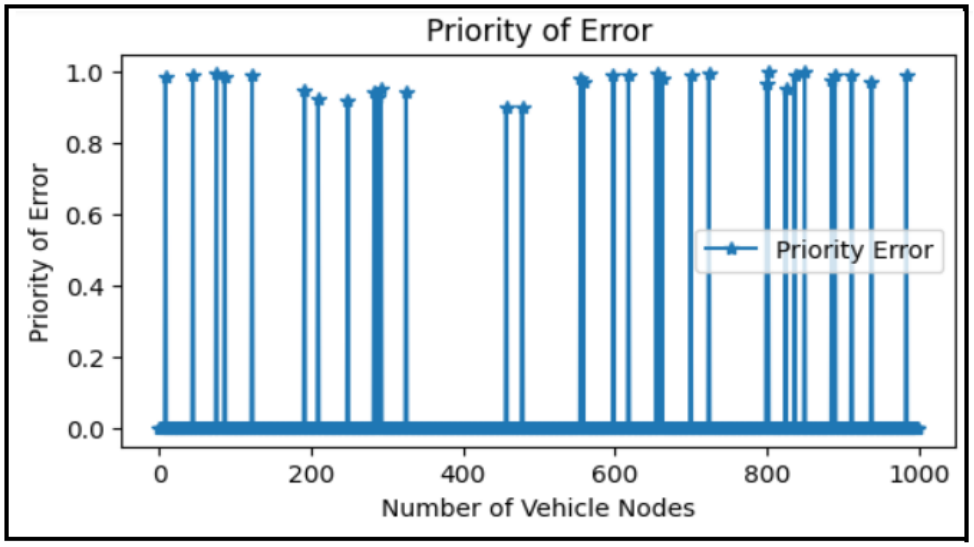


Figure 11. Priority of Error Nodes from 1000 Vehicle Nodes

8.1. Impact of TPBFT on Fault Tolerance

In case of a protocol failure, the network self-heals between two conflicting rounds of the protocol. A newly connected node experiencing a protocol failure would, when choosing from different known peers to connect to, pick similarly behaving nodes. The network would then heal, declaring the unknown link bandwidth performance peer node as a malicious misbehaving node, hence limiting its ability to participate in the protocol consensus. This means that if a known peer is trying to sybil attack a node, it would do so with already known misbehaving sybil nodes, being unable to mask its capabilities. Upon being flooded with vote messages showing the Byzantine misbehaving node signature for a consensus slot, previously known settled and accepted

messages showing a different signature by a majority are validated as correct, and this can happen locally. Newly connected nodes should be untrusted until discovered as not being Sybil partners of a peer-connected node.

However, during the presence of the adversary's conflicting vote broadcast, some unknown remote nodes may open connections that ask for part of an attacker's signed vote. If the nodes identify signature misuse by the possible Byzantine adversaries, they receive votes from, they can quickly declare the newly connected nodes as attackers, hence dropping them as connected peers. During this broadcast, connected peers can locate other malicious peers since there will not be agreement with their view over the decision that has been settled and accepted. It is only because the unknown connected nodes may behave without knowing current vote round results, which in some cases can be valid syntactic actions that cost bandwidth over the network. With only broadcast messages from nodes in the view, only two-thirds of nodes need to receive vote messages to achieve the topology convergence of interconnected peers, ensuring the success of the protocol, as shown in Figure 12.

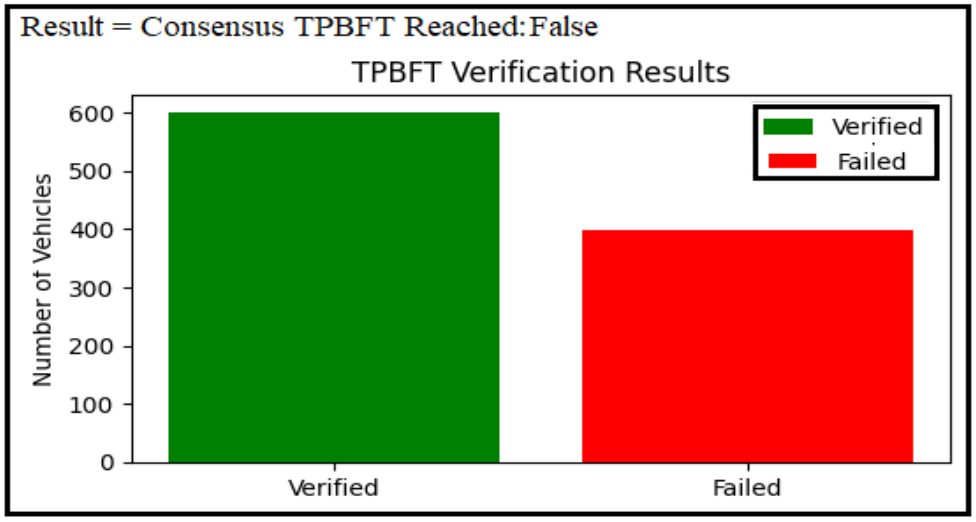


Figure 12. The Total TPBFT Verification of 1000 Vehicle Nodes

9. DISCUSSION AND FUTURE WORK

Discussions on the findings are followed by potential ideas for future work in this chapter. This chapter concludes with a summary of the relation of each research objective to the findings and a forecast about the development of the AVs and VANET environment.

The implementations simulated that as VANET was applied, the security and reliability of the PBFT and TBFT systems were enhanced. We projected that the nodes for keeping and protecting the blockchain technology would move and develop along with the AVs, reflecting the result of our research on SMC. Additionally, numerous vehicles would host their copies of the blockchain technology before the wave of AVs shows up on the road. The capability of two-way communication among civilian cars would both increase trust in traffic safety and promote the public adoption of the AVs. More extensive data in VANET systems and security and reliability in VANET systems may upgrade the effectiveness of blockchain technology. After the wave of AVs we projected, numerous vehicles would host their copies of the blockchain technology. Therefore, the capability of two-way communication among civilian cars would both increase trust in traffic safety and promote the public adoption of the AVs. More extensive data in VANET systems and security and reliability in VANET systems may upgrade the effectiveness of blockchain technology.

9.1. Limitations and Potential Improvements

We developed a VANET system-based VANT and blockchain. We presented two methods that the VANET system can benefit a blockchain system. As to the first method, the PBFT or TBFT algorithm is used to construct and maintain the blockchain system in each vehicle at every time period; as a result, they can achieve a faster consensus. As to the second method, the PBFT or TBFT algorithm is used to construct the blockchain system when some vehicles arrive at the destination. Making use of both of them should be a better choice than using the singular.

Although our proposal showed the advantages, it still has some limitations that are waiting for improvement. We plan to improve the following areas in the future: a) Set the electric device in the vehicle

on/off. After the engine is ignited, electricity is available; otherwise, it is not available. We will utilize private vehicle owners to maintain their own blockchain system because the power supply of each vehicle connected to the public service is very limited. There could be a huge obstacle if the current is used to maintain the blockchain system. Also, in fact, the RID of each vehicle is a unique code, which has a relationship with the initialization function and cannot be 0. That is to say, the vehicle communicates with its destination at any time. The decision-making function of the vehicle must be started at any moment. However, whether it is started or not has nothing to do with whether the engine is on or not. The function is constant.

10. CONCLUSION

This research presented a comprehensive investigation into enhancing Vehicular Ad hoc Networks (VANETs) through the integration of an improved consensus mechanism tailored for dynamic, adversarial environments. Our work centered on the design, implementation, and evaluation of a **Trust Practical Byzantine Fault Tolerance (TPBFT)** protocol, specifically engineered to address the critical challenges of latency and fault tolerance in blockchain-based vehicular systems.

Research Summary

Through realistic simulations employing the SUMO traffic simulator and OpenStreetMap data, we demonstrated that TPBFT significantly outperforms traditional PBFT within VANET contexts. The proposed mechanism achieved a marked reduction in consensus latency, reaching as low as 16-28 milliseconds, while maintaining robust operation in the presence of malicious nodes. These results validate TPBFT as a viable and efficient consensus layer for secure, decentralized communication in intelligent transportation systems.

Key Contributions

The primary contributions of this paper are threefold:

1. **A Novel Consensus Protocol:** We designed TPBFT, which incorporates dynamic trust evaluation and optimized communication phases to reduce overhead and accelerate consensus formation in mobile networks.
2. **A High-Fidelity Evaluation Framework:** We established a complete simulation ecosystem that models real-world urban mobility and network conditions, providing a reliable testbed for consensus protocol analysis in VANETs.
3. **Empirical Performance Validation:** We conducted a rigorous comparative analysis, quantifying TPBFT's advantages over PBFT in terms of latency, throughput, and resilience against Byzantine failures.

Limitations and Future Work

Despite promising results, our study acknowledges certain limitations. The simulations, while realistic, operate under controlled network assumptions and idealized traffic models. Furthermore, the energy consumption associated with continuous consensus operations and the scalability of the protocol in ultra-dense vehicular scenarios require deeper exploration.

Our future research will focus on the following directions:

1. **Energy-Efficient TPBFT:** Developing an adaptive version of TPBFT that optimizes for power consumption, crucial for vehicle-mounted hardware with limited energy budgets.
2. **Enhanced Security Layers:** Investigating and integrating advanced cryptographic techniques, such as lattice-based encryption or lightweight homomorphic computation, for end-to-end data protection within the blockchain ledger.
3. **Real-World Prototyping:** Transitioning from simulation to a hardware testbed using standard On-Board Units (OBUs) and Road-Side Units (RSUs) to validate system performance under physical layer constraints and real-channel impairments.
4. **Dynamic Coordinator Election:** Refining the leader election mechanism to be more robust and efficient during frequent network topology changes, thereby improving overall system stability and throughput.

In summary, this work provides a foundational step toward secure, low-latency, and trustworthy cooperative systems for the future of intelligent transportation. By bridging the gap between robust blockchain consensus and the demanding environment of VANETs, our TPBFT protocol paves the way for the reliable and large-scale deployment of decentralized automotive applications.

REFERENCES

[1] P. Sapkale, S. Mehta, and S. Balamurugan, *Quantum Computing and Machine Learning for 6G*. John Wiley & Sons. 2026, https://doi.org/10.1002/9781394238118.

[2] G. Singh, S. Sharma, A. K. J. Saudagar, and S. Kumar, "A secure group-based authentication protocol for IoVT in 5G-enabled smart transportation and road safety systems," *Scientific Reports,* 2026, https://doi.org/10.1038/s41598-025-31123-w.
[3] T. D. Nguyen, N. A. Tong, B. P. Nguyen, Q. V. Hung Nguyen, P. L. Nguyen and T. T. Huynh, "Hierarchical Federated Learning in MEC Networks with Knowledge Distillation," *2024 International Joint Conference on Neural Networks (IJCNN)*, pp. 1-8, 2024, https://doi.org/10.1109/IJCNN60899.2024.10651323.
[4] L. Qudus, "Resilient systems: building secure cyber-physical infrastructure for critical industries against emerging threats," *Int J Res Publ Rev,* vol. 6, no. 1, pp. 3330-46, 2025, https://doi.org/10.55248/gengpi.6.0125.0514.
[5] N. Canino, P. Dini, S. Mazzetti, D. Rossi, S. Saponara, and E. Soldaini, "Cybersecurity of automotive wired networking systems: evolution, challenges, and countermeasures," *Electronics*, vol. 14, no. 3, p. 471, 2025, https://doi.org/10.3390/electronics14030471.
[6] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions," *ACM Computing Surveys,* vol. 56, no. 10, pp. 1-39, 2024, https://doi.org/10.1145/3656166.
[7] R. Sarpong, F. Araújo, and B. Sousa, "The potential of SDNs and multihoming in VANETs: A Comprehensive Survey," in *2025 12th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 265-272, 2025, https://doi.org/10.1109/FiCloud66139.2025.00043.
[8] A. J. Albarakati, "Blockchain-Based Trust Management Framework Using Spiking Neural Networks for 6G-Enabled IoT Ecosystems: A Secure Approach for Intelligent Transportation Systems," *Journal of Circuits, Systems and Computers,* p. 2642010, 2026, https://doi.org/10.1142/S0218126626420107.
[9] Z. Ullah *et al.*, "TrustChain-VANETs: Blockchain and IPFS Integration for Reliable and Secure Vehicular Communication in Intelligent Transportation Systems (ITS)," *IET Intelligent Transport Systems,* vol. 19, no. 1, p. e70051, 2025, https://doi.org/10.1049/itr2.70051.
[10] A. Fujihara, "Exploring the universality of finality time in proof-of-stake blockchains: empirical analysis and mathematical formulation of size-synchrony antagonism," in *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1-5, 2025, https://doi.org/10.1109/ICBC64466.2025.11114702.
[11] Y. Xu, Y. Lei, L. Tang, X. Li, and Z. Sun, "A Hybrid Consensus Optimization Algorithm for Blockchain in Supply Chain Traceability," *Electronics,* vol. 15, no. 1, p. 77, 2025, https://doi.org/10.3390/electronics15010077.
[12] S. Khokha, "Integrating safety and security in autonomous vehicles: a comprehensive review," In *2024 4th International Conference on Sustainable Expert Systems (ICSES)*, pp. 460-464 2024, https://doi.org/10.1109/ICSES63445.2024.10763275.
[13] N. Dasanayaka, K. F. Hasan, C. Wang, and Y. Feng, "Enhancing vulnerable road user safety: A survey of existing practices and consideration for using mobile devices for V2X connections," *arXiv preprint arXiv:2010.15502*, 2020, https://doi.org/10.48550/arXiv.2010.15502.
[14] 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 & Tutorials,* vol. 24, no. 2, pp. 1212-1239, 2022, https://doi.org/10.1109/COMST.2022.3160925.
[15] X. Li, W. Jiang, W. Wang, T. Zhou, K. Wang, and S. Liu, "Joint channel connectivity and interference management in DT-assisted cognitive vehicular networks," *Ad Hoc Networks,* vol. 183, p. 104094, 2026, https://doi.org/10.1016/j.adhoc.2025.104094.
[16] A. Gheysari and H. R. Zarandi, "Security-aware optimization of PoW-based blockchain performance using a genetic algorithm approach," *Sustainable Computing: Informatics and Systems,* p. 101232, 2025, https://doi.org/10.1016/j.suscom.2025.101232.
[17] D. Jia, G. Yang, M. Huang, J. Xin, G. Wang, and G. Y. Yuan, "An efficient privacy-preserving blockchain storage method for internet of things environment," *World Wide Web,* pp. 1-18, 2023, https://doi.org/10.1007/s11280-023-01172-0.
[18] S. Tang, Z. Wang, J. Jiang, S. Ge, and G. Tan, "Improved PBFT algorithm for high-frequency trading scenarios of alliance blockchain," *Scientific Reports,* vol. 12, no. 1, p. 4426, 2022, https://doi.org/10.1038/s41598-022-08587-1.
[19] S. B. A. Bukhari, H. Albalawi, A. Wadood, and A. M. Alatwi, "Deep learning-driven fault detection and classification in microgrids using Temporal Convolutional Network," *Computers and Electrical Engineering,* vol. 129, p. 110777, 2026, https://doi.org/10.1016/j.compeleceng.2025.110777.
[20] A. Behura, A. Kumar, and P. K. Jain, "A comparative performance analysis of vehicular routing protocols in intelligent transportation systems," *Telecommunication Systems*, vol. 88, no. 1, p. 26, 2025, https://doi.org/10.1007/s11235-024-01243-1.
[21] H. Wu, C. Yue, L. Zhang, Y. Li, and M. A. Imran, "When Distributed Consensus Meets Wireless Connected Autonomous Systems: A Review and A DAG-based Approach," *IEEE Network,* vol. 39, no. 1, pp. 261-269 2024, https://doi.org/10.1109/MNET.2024.3482273.
[22] O. B. Akinola, "Comparative Insights On The Legal Status Of Cryptocurrencies: Lessons For Uganda," *The Nnamdi Azikiwe University Journal of Commercial and Property Law,* vol. 13, no. 1, 2026, https://journals.ezenwaohaetorc.org/index.php/NAUJCPL/article/view/3593.
[23] J. K. Adeniyi *et al.*, "A biometrics-generated private/public key cryptography for a blockchain-based e-voting system," *Egyptian Informatics Journal,* vol. 25, 2024, https://doi.org/10.1016/j.eij.2024.100447.

[24] C. Delgado-von-Eitzen, M. J. Fernández-Iglesias, L. Anido-Rifón, and F. A. Mikic-Fonte, "Blockchain beyond immutability: Application firewalls on ethereum-based platforms," *Computer Standards & Interfaces,* vol. 95, p. 104038, 2026, https://doi.org/10.1016/j.csi.2025.104038.
[25] M. A. Shawky *et al.*, "Blockchain-based secret key extraction for efficient and secure authentication in VANETs," *Journal of Information Security and Applications,* vol. 74, p. 103476, 2023, https://doi.org/10.1016/j.jisa.2023.103476.
[26] Y. Xie, C. Tang, Z. Chen, J. Lai, Z. Zheng, and X. Yu, "Towards proof-of-prospect consensus mechanism for maximizing consumers' satisfaction in distributed energy systems," *Science China Information Sciences,* vol. 69, no. 2, p. 122202, 2026, https://doi.org/10.1007/s11432-024-4438-5.
[27] A. Dutta, L. M. Samaniego Campoverde, M. Tropea, and F. De Rango, "A comprehensive review of recent developments in vanet for traffic, safety & remote monitoring applications," *Journal of Network and Systems Management,* vol. 32, no. 4, p. 73, 2024, https://doi.org/10.1007/s10922-024-09853-5.
[28] V. Alagappan, "A Governance Model for IoT Data in Global Manufacturing," *arXiv preprint arXiv:2601.09744*, 2026, https://doi.org/10.48550/arXiv.2601.09744.
[29] M. G. Xevgenis, M. Polychronaki, D. G. Kogias, H. C. Leligkou, and E. Liotou, "Securing Zero-Touch Networks with Blockchain: Decentralized Identity Management and Oracle-Assisted Monitoring," *Electronics,* vol. 15, no. 2, p. 266, 2026, https://doi.org/10.3390/electronics15020266.
[30] P. Selvaprabhu, "An examination of distributed and decentralized systems for trustworthy control of supply chains," *IEEE access,* vol. 11, pp. 137025-137052, 2023, https://doi.org/10.1109/ACCESS.2023.3338739.
[31] M. Stephens, "Enhancing Global Cybersecurity Resilience: Navigating the Subconscious Fallacies within Critical Infrastructure Protection," *Journal of Information Warfare,* vol. 23, no. 3, pp. 82-94, 2024, https://doi.org/10.34190/eccws.23.1.2213.
[32] K. Sharma, K. Bhatt, and I. Giri, "Regulatory Migration to Europe: ICO Reallocation Following US Securities Enforcement," *arXiv preprint arXiv:2602.00138*, 2026, https://doi.org/10.48550/arXiv.2602.00138.
[33] N. S. Liqaa Saadi Mezher, Dheyaa Jasim Kadhim, "Load Balancing Based Intelligent Software Defined Networking (SDN) Controller," *Journal of Information Systems Engineering and Management,* vol. 10, no. 1, pp. 57 - 68, 2025, https://doi.org/10.52783/jisem.v10i1s.101.
[34] N. M. Nasir, S. Hassan and K. Mohd Zaini, "Securing Permissioned Blockchain-Based Systems: An Analysis on the Significance of Consensus Mechanisms," in *IEEE Access*, vol. 12, pp. 138211-138238, 2024, https://doi.org/10.1109/ACCESS.2024.3465869.
[35] K. W. Lin, Y.-J. Zheng, J.-C. Chen, W.-C. Wang, and C.-C. Chen, "A parallel and distributed C4. 5 algorithm in cloud computing environments," *Computing,* vol. 107, no. 2, pp. 1-38, 2025, https://doi.org/10.1007/s00607-025-01415-0.
[36] J. A. R. de Souza, E. R. Cavalcanti, T. de Sales Bezerra, and R. C. d. M. Gomes, "VANETs' research overview updated: past, present and future," *Journal of the Brazilian Computer Society,* vol. 30, no. 1, pp. 380-393, 2024, https://doi.org/10.5753/jbcs.2024.3354.
[37] L. S. Mezher, "An Overview on Vehicular Ad Hoc Networks Security," *Journal of Engineering Research and Reports,* vol. 28, no. 1, pp. 189-204, 2026, https://doi.org/10.9734/jerr/2026/v28i11769.
[38] R. Wang *et al.*, "Parallel Byzantine fault tolerance consensus based on trusted execution environments," *Peer-to-Peer Networking and Applications,* vol. 18, no. 1, p. 31, 2025, https://doi.org/10.1007/s12083-024-01830-8.
[39] B. L. Nguyen, D. T. Ngo, and H. L. Vu, "Vehicle Communications for Infotainment Applications," In *Handbook of Real-Time Computing*, pp. 705-722, 2022, https://doi.org/10.1007/978-981-287-251-7_44.
[40] L. S. Mezher and M. H. Saleh, "Enhancing VANET Security using Blockchain and SHA3-256 in Python," *Journal of Studies in Science and Engineering,* vol. 5, no. 1, pp. 84-109, 2025, https://doi.org/10.53898/josse2025515.
[41] J. Ghosh, N. Kumar, K. A. Al-Utaibi, S. M. Sait, V. N. Vo, and C. So-In, "Reliable data transmission for a VANET-IoIT architecture: A DNN approach," *Internet of Things,* vol. 25, p. 101129, 2024, https://doi.org/10.1016/j.iot.2024.101129.
[42] N. Wang *et al.*, "Application of the BCT Model Based on Process and Behavioral Interventions to Improve the Quality of Blood Culture Collection," *Infection Prevention in Practice,* p. 100509, 2026, https://doi.org/10.1016/j.infpip.2026.100509.
[43] E. Ngatunga, M. Kissaka, and A. T. Abdalla, "Performance evaluation of cluster-based schemes for message dissemination in a vehicle-to-vehicle communication in urban environment," *Cogent Engineering,* vol. 11, no. 1, p. 2348885, 2024, https://doi.org/10.1080/23311916.2024.2348885.
[44] M. Soori, F. K. G. Jough, R. Dastres, and B. Arezoo, "Blockchains for industrial Internet of Things in sustainable supply chain management of industry 4.0, a review," *Sustainable Manufacturing and Service Economics,* vol. 3, p. 100026, 2024, https://doi.org/10.1016/j.smse.2024.100026.
[45] A. Kumar, L. Vishwakarma, and D. Das, "R-PBFT: A secure and intelligent consensus algorithm for Internet of vehicles," *Vehicular Communications,* vol. 41, p. 100609, 2023, https://doi.org/10.1016/j.vehcom.2023.100609.
[46] A. Alshahrani *et al.*, "An Intelligent Latency Aware DDoS Detection Framework for Secure Vehicular Ad Hoc Networks," *Transactions on Emerging Telecommunications Technologies,* vol. 37, no. 1, p. e70348, 2026, https://doi.org/10.1002/ett.70348.

[47] S. BK and F. Azam, "Ensuring security and privacy in vanet: A comprehensive survey of authentication approaches," *Journal of Computer Networks and Communications,* vol. 2024, no. 1, p. 1818079, 2024, https://doi.org/10.1155/2024/1818079.

[48] O. Q. Wu, R. Kapuscinski, and S. Suresh, "On the distributed energy storage investment and operations," *Manufacturing & Service Operations Management,* vol. 25, no. 6, pp. 2277-2297, 2023, https://doi.org/10.1287/msom.2020.0652.

[49] S. Mondal, K. Dogra, S. Gupta, and S. K. Gupta, "A Blockchain-Based OBD Architecture for Secure Data Sharing in Smart Vehicle Ecosystems," *Security and Privacy,* vol. 9, no. 1, p. e70158, 2026, https://doi.org/10.1002/spy2.70158.

[50] A. Shahidinejad, J. Abawajy, and S. Huda, "Anonymous lattice-based authentication protocol for vehicular communications," *Vehicular Communications,* vol. 48, 2024, doi: 10.1016/j.vehcom.2024.100803, https://doi.org/10.1016/j.vehcom.2024.100803.

[51] J. A. Alzubi, N. R. Lavuri, K. Dharavath, N. Nallameti, S. Venugopal, and P. Palanisamy, "A Secure Authentication and Task Offloading Model Using Blockchain-Assisted Hybrid Serial Learning in Multiaccess Edge Computing for Vehicular Ad Hoc Networks Sector," *International Journal of Communication Systems,* vol. 39, no. 3, p. e70382, 2026, https://doi.org/10.1002/dac.70382.

[52] R. Bala, R. Manoharan, and G. Ramya, "Trust models for blockchain networks: a comprehensive review," *Journal of Ambient Intelligence and Humanized Computing,* pp. 1-20, 2026, https://doi.org/10.1007/s12652-025-05027-6.

[53] J. Grover, "Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review," *Vehicular Communications*, vol. 34, p. 100458, 2022, https://doi.org/10.1016/j.vehcom.2022.100458.

[54] A. A. Al-awamy, N. Al-shaibany, A. Sikora, and D. Welte, "Hybrid Consensus Mechanisms in Blockchain: A Comprehensive Review," *International Journal of Intelligent Systems,* vol. 2025, no. 1, p. 5821997, 2025, https://doi.org/10.1155/int/5821997.