ORIGINAL ARTICLE
Electrica 2026; 26: 1-15

Addressing Network Management Challenges in Vehicle-to-Vehicle Communication Through Consortium Blockchain and Proof of Authority

Şükrü Okul[1,2], Fatih Keleş[2]

[1]Tübitak Bilgem, Kocaeli, Türkiye
[2]Department of Computer Engineering, İstanbul University-Cerrahpaşa Faculty of Engineering, İstanbul, Türkiye

Cite this article as: Ş. Okul and F. Keleş, "Addressing network management challenges in vehicle-to-vehicle communication through consortium blockchain and proof of authority," *Electrica*, 26, 0426, 2026. doi: 10.5152/electrica.2026.25426.

WHAT IS ALREADY KNOWN ON THIS TOPIC?

- *Traditional vehicle-to-vehicle (V2V) communication systems rely on centralized cloud servers, leading to scalability issues, bottlenecks, and the risk of a single point of failure.*
- *Data integrity and user privacy are critical in V2V networks; however, current security methods struggle to balance speed and security in high-mobility environments.*
- *Blockchain technology is often proposed as a solution for ensuring data integrity in distributed systems. However, traditional consensus algorithms such as Proof of Work (PoW) introduce high latency. This limitation makes them unsuitable for rapidly changing traffic environments.*

Corresponding author:
Şükrü Okul

E-mail:
sukru.okul@tubitak.gov.tr, sukruokul@gmail.com

Received: January 14, 2026
Revision Requested: March 11, 2026
Last Revision Received: March 18, 2026
Accepted: March 27, 2026
Publication Date: September 25, 2026

DOI: 10.5152/electrica.2026.25426

Content of this journal is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

ABSTRACT

This study addresses critical challenges in vehicle-to-vehicle (V2V) communication systems by leveraging blockchain technology combined with the Proof of Authority (PoA) consensus algorithm. The research focuses on four major issues: centralized system dependencies, communication inefficiencies in highly mobile environments, data integrity, and privacy concerns. To tackle dependency issues prevalent in centralized systems, a decentralized blockchain architecture is proposed. This architecture mitigates security risks and management complexities associated with centralized models, thereby enhancing overall system robustness. In the context of V2V communication, where rapid and efficient data exchange is essential, a consortium blockchain is advocated. This choice is aimed at optimizing communication efficiency and minimizing data loss, particularly during simultaneous data requests in highly dynamic environments. The immutable nature of blockchain technology is employed to address data integrity concerns. By ensuring that all transactions are recorded in a tamper-proof ledger, blockchain eliminates the need for centralized update processes, thereby preserving data accuracy. Privacy issues are addressed through the implementation of public-private key pairs within the consortium blockchain framework, which safeguards user data against unauthorized access. Additionally, the PoA consensus algorithm is utilized to enhance system performance and prevent data loss. The algorithm's efficiency is demonstrated through a queue mechanism that ensures reliable transaction processing. Performance evaluations, including simulations and mathematical analyses, highlight significant improvements in efficiency compared to existing models. This study provides a novel solution that balances speed and security in decentralized V2V communication networks. It advances the state-of-the-art in network management by integrating blockchain technology with PoA, contributing valuable insights and practical solutions to the field. Simulation results indicate that the proposed model reduces the average transaction waiting time to approximately 14.98 ms, demonstrating improved efficiency compared to existing V2V communication architectures.

Index Terms— Blockchain-based V2V networks, consortium blockchain, data integrity, V2V communication

I. INTRODUCTION

In this section, detailed theoretical information is given by mentioning the relationship between blockchain and vehicle-to-vehicle (V2V) communication. Communication between vehicles is becoming more important every day. At the same time, V2V communication has many advantages and disadvantages in terms of security and speed. Many studies attempt to integrate various technologies into this communication. The most current of these technologies is blockchain technology. This technology is also utilized in the present work. However, problems may arise in systems with high mobility. In order to prevent these problems, a consortium blockchain and a queue structure have been added to the system.

Communication between highly mobile elements, such as vehicles, is an important problem as it requires high performance and reliability. Achieving safety and performance at the same time is a difficult phenomenon. For this reason, it is important to communicate between vehicles, that

WHAT DOES THIS STUDY ADD ON THIS TOPIC?

- *It offers a fully decentralized consortium blockchain architecture that eliminates the need for roadside units and utilizes the vehicles' own wireless technology.*
- *It proposes a unique structure that integrates the Proof of Authority consensus algorithm with a queue-based transaction pool to improve system performance and prevent data loss.*
- *The proposed model was validated using mathematical queue theory analysis. The results demonstrate higher efficiency compared to existing studies. The average waiting time was reduced to 14.98 miliseconds during the simulation tests..*

is, to use vehicular ad-hoc networks (VANET) and blockchain together. The reason for this is the data integrity and security provided by the blockchain, and the performance can be provided according to the blockchain algorithm to be used. In this study, data integrity and data security are examined while building a secure model. Preventing data corruption and ensuring its integrity is a top priority.

Traditional security and privacy methods used in V2V communication tend to be ineffective due to the challenges of centralization, lack of privacy, and security threats. Centralization: Current smart vehicle architectures are based on centrally-mediated communication models where all vehicles are identified, authenticated, authorized, and connected via centralized cloud servers. This model is unlikely to scale because so many tools are interconnected. Additionally, cloud servers remain a bottleneck and a single point of failure that can disrupt the entire network. Lack of privacy: It is another important challenge in vehicular communication systems. Many existing secure communication architectures do not adequately consider user privacy. In some cases, the entire vehicle data is shared without the owner's consent, while in others only noisy or summarized data is provided to the requester. However, in many smart vehicle applications, the requester needs precise vehicle data to provide personalized services. Security threats: There are an increasing number of autonomous driving functions in smart vehicles. A malfunction resulting from a security breach (e.g., due to the installation of malware) can cause serious accidents, endangering the safety of passengers and other nearby road users [1].

Blockchain technology has recently attracted significant attention from international organizations, the private sector, and public institutions. Some researchers even describe blockchain as a technology that could become as transformative as the Internet [2]. From an academic perspective, studies on blockchain technology were relatively limited in the past. However, the number of studies in this field has increased significantly in recent years [3]. The most important reason for using blockchain technology in this study is that it is the technology that best ensures and guarantees data integrity. The accuracy of the data used in this technology is certain if the system is not compromised by malicious software or the system [4-5].

In the system, the roadside unit (RSU) is eliminated through the use of blockchain and the connected car. Additionally, a structure supporting both V2V and V2I communication is implemented. Data integrity is ensured through the blockchain integrated into the system. Here, integrity is maintained using public and private keys along with the ledger located at each decision node. The primary challenge is to maintain acceptable performance without data loss in a highly mobile system. A contribution in this area is achieved by employing a queuing model that considers both performance and data loss. In the test results section, the effect of the number of consortium nodes on acceptable performance, relative to system density, is presented.

Wireless technologies used in VANET include cellular networks, wireless local area network/wireless fidelity, Worldwide Interoperability for Microwave Access (WiMAX), and Dedicated Short-range Communications (DSRC). Worldwide Interoperability for Microwave Access technology provides high-quality service and reliable communication standards, making it suitable for applications requiring multimedia and video. Wireless technologies like WiMAX can support both V2V and V2I communication. In DSRC, V2V and V2I communication is facilitated through other wireless technologies. The primary purpose of DSRC is to minimize communication delay during data exchange. It enables vehicles to transmit critical information, such as traffic conditions, accidents, and road status, while maintaining high data transmission rates [6].

As indicated by the discussed VANET-related information, communication in this domain is conducted via wireless technologies. In this paper, it is assumed that wireless communication occurs optimally and that vehicles can communicate effectively based on the information presented above.

The most challenging part of the VANET is the disruption of communication due to high mobility. This is due to RSUs in existing systems. The limited coverage area of RSUs creates additional challenges for vehicular communication systems. In addition, vehicle density around each RSU is often uneven, which negatively affects communication reliability. To solve all these problems, a fast system is used over light encryption, in which the vehicles' wireless sensors are used. While security is provided by encryption in existing systems, blockchain technology is used in the proposed model.

Blockchain technology can be defined as a distributed ledger architecture. Theoretically, it can be thought of as using the notebook pages of the system. The pages of the notebook are filled by the users of the notebook. All filled-in information continues to be found on the previous pages of the book without being deleted or corrupted. Unlike traditional ledgers, in the blockchain, each page is linked to the next page by an encrypted hash algorithm, and the direction of data flow to the ledger is always forward [7].

Many researchers are working on blockchain. Each researcher has many comments on this issue. Reyna offers a distributed, traceable, immutable, and secure data structure, where the reliability of the transactions using blockchain technology is verified by the stakeholders in the connected network [8]. Glaser describes blockchain as a database shared within a network determined by its users, where the records of critical information are maintained without the need of a central authority, that is, independently accessible by all participants and using pseudonyms [9]. Zheng, on the other hand, defines this technology as a big data ledger where all transactions are recorded in blocks that grow as new blocks are added [10]. According to Nakamoto, blockchain technology is a distributed data structure in which transaction information is stored by other participants and shared across the network [11]. According to Beck, blockchain technology is a data set that provides consistent transactions through interaction with a large number of nodes, or participants, in the network where it is located and produced by itself [12]. Tama defines blockchain as a component of a distributed software system aimed at ensuring data integrity [13].

Some researchers focus only on data integrity without considering the detailed aspects of the blockchain. For example, Halpin defines the blockchain as only a cryptographically verifiable list of data [14]. From a technical perspective, blockchain can be described as a distributed database, a mechanism that does not need an independent, centralized structure, and a combination of algorithms used for cryptographic encryption and hashing mechanisms. Transaction data used in blockchain technology is interconnected using encryption algorithms and stored in an endless array of data blocks with potential for use. The formation of these blocks is validated through voting by participating nodes using decentralized timestamped algorithms to ensure accuracy and validity of transactions [15]. Zhao's study shows that the most important feature of the blockchain is its ability to provide reliable and transparent transactions through network-based computations rather than human intervention [16]. With this feature, the blockchain can be expressed as "an operating system for interactions" [17]. According to Lewis, the main difference between blockchain technology and traditional databases is that blockchain technology is a highly advanced type that can provide rules-based solutions by working on the peer-to-peer network for operations such as adding new data, verifying the added information, and sharing the information database [18].

Data integrity is a very important security problem. The most important factor in the emergence of blockchain systems is the difficulty of ensuring data integrity. In the proposed architecture, data integrity is guaranteed by using blockchain technology. Public and private keys are used for the security of messaging. Cryptography details in the messaging section will be discussed in the system design section.

Existing blockchain systems are classified into three categories: public blockchain, private blockchain, and consortium blockchain [19]. A public blockchain is a type of blockchain in which all nodes are involved in the approval process, and information can become part of the chain after at least more than half of them are approved in the approval mechanism [20].

The consortium blockchain used in the system can be defined as a partially private and permitted blockchain structure, where a predetermined and selected group of nodes serve as decision-makers, rather than a single structure, in processes such as verifying each block in the blockchain and consensus. These designated nodes determine which participants may join the blockchain network and which participants are permitted to mine data. For each block verification in the blockchain, a multi-signature scheme is used when it is sufficient to sign the relevant block only by authorized nodes. The consortium also determines whether the network is public or limited and whether all participants have read and write access to the data. [19-20].

Because the blockchain is decentralized, it relies heavily on a consensus mechanism to validate transactions on the blockchain. Also, the speed of consensus depends on the type of consensus method used, with some consensus methods being faster than others. Common consensus methods include Proof of Work (PoW), Proof of Stake (PoS), and Proof of Authority (PoA) [19-21].

Proof of Authority has several important advantages over other consensus methods. It is more scalable because it has a certain number of block validators compared to PoW and PoS methods. In PoA, blocks are validated using digital IDs (identification numbers) rather than the amount of cryptocurrency held, thereby relying on validator reputation. The interval for generating new blocks can also be estimated more accurately, whereas this interval varies in PoW and PoS systems. In addition, PoA provides a high transaction rate.

Considering all the mentioned blockchains and their algorithms, the consortium blockchain and PoA consensus algorithms were selected for this study due to their advantages. This queue structure and PoA algorithm are used to contribute to the paradox of speed and security in the consortium blockchain. The implementation of this algorithm is explained in Section 3.

The primary reason for adopting a blockchain-based system, as mentioned before, is the requirement for transactions to be conducted in a decentralized manner. This decentralization eliminates the need for costly mechanisms such as RSU. Finally, the most important reason for using the PoA consensus mechanism together with the consortium blockchain is to prevent data loss in the system and prevent it from entering a bottleneck.

The main contributions of this study can be summarized as follows:

- A consortium blockchain architecture specifically designed for secure and efficient V2V communication systems is proposed.
- A queue-based transaction management mechanism integrated with the PoA consensus algorithm is introduced to reduce transaction waiting time and improve system reliability.
- The proposed model addresses the high mobility problem in vehicular networks by enabling vehicles to communicate directly through wireless technologies without relying heavily on RSU infrastructure.

- Mathematical queue theory analysis is used to evaluate the performance of the proposed architecture and demonstrate improvements in transaction processing efficiency.
- Simulation results show that the proposed model achieves reduced transaction waiting times and improved system performance compared to existing blockchain-based vehicular communication approaches.

II. PREVIOUS WORKS

Blockchain-related studies have been conducted in many fields, attracting considerable attention from researchers because of the growing relevance of this technology. Blockchain-based systems are increasingly integrated with other technologies such as the Internet of Things, smart airports, smart healthcare, and security systems to improve efficiency, usability, and reliability [21-26]. Source verification [27], trust and reputation management [28], event and message exchange management [29], use of smart payment [30], and traffic inspection [31] are some of the fields used to achieve similar advantages to ensure security.

Several studies have suggested various authentication methods to ensure the authenticity of the Internet of Vehicles (IoV) in existing systems. Some studies propose the use of a Certificate Authority (CA) to authenticate IoVs, while others incorporate blockchain for authentication, this CA is a central body. In other words, this is an indication of the existence of a trusted authority. For example, Lai presents a study to increase the efficiency of the authentication process using blockchain technology, blocks, and to share information between router-control databases [32]. In another study, Javaid authenticates using the CA, that is, the central authority, and uses blockchain technology to store the authentication information there, but they do not mention the overheads brought to the system here [33]. In another study, to develop a smart payment system, not only the tools, but also the trust information of the infrastructure are stored in a blockchain, and before any transaction, both the cashier and the driver are checked for each other's authenticity, and the transaction information is also stored in the blockchain [29]. Ali, in another study, uses several blockchains to separately store authorized and unauthorized vehicle information [34]. In addition, Ali proposes a certificate-less authentication protocol to eliminate the overhead of the certificate-based system. In two other similar studies, two different blockchains are used: one is used to store the information of certified and revoked vehicles, while another blockchain is used to store the messages resulting from communication between vehicles [35]. Zhang, on the other hand, stores blockchain technology in a blockchain-based storage system, along with authentication information, location, and direction information, and additionally adds all rule violations to the blockchain to store reputation information [36]. As certificate creation, signing, and verification bring high overhead, storing authentication information and protecting the confidentiality of blockchain tools are used in another study [37]. However, in this work, which gains this advantage, the method of increasing security services creates a high computational load. Similarly, in some other studies, many protocols require too much time and computational overhead to complete the authentication processes [38–40]. Also, a method proposed by Li et al. and Salem et al. requires a lot of storage space to store the authentication information of vehicles [41-42]. Luo et al. propose an efficient and stable authentication method supported by hierarchical blockchain and fog computing as a solution to the challenging authentication problem in the IoVs [43]. Yang et al. analyzed the relationship between PBFT consensus success rate and delay in the ideal channel of IoV [44].

Based on the RSU, all of the above-mentioned protocols require expensive infrastructure support. In addition, traditionally used certificate-based protocols create a higher overhead in areas where they have started to use extra features in classical blockchain technology, along with parts with lightweight encryption where they create less overhead by using blockchain technology [27].

Recently, blockchain-based vehicular communication architectures have gained significant attention for improving trust management and security in dynamic vehicular environments. For instance, Khan et al. proposed a blockchain-based framework for secure vehicle communication that enables decentralized authentication and secure message exchange between vehicles without relying on centralized authorities [45].

Similarly, Wang et al. introduced a lightweight blockchain architecture for IoV environments that improves scalability and reduces transaction latency by using efficient consensus mechanisms [46].

In another recent study, Zhou et al. investigated blockchain-enabled V2V communication models and demonstrated that decentralized blockchain infrastructures can significantly enhance data integrity and reliability in vehicular networks [47].

In all these previous studies, security was provided by encryption algorithms with high execution times due to the transactions made over the RSU. In addition, high mobility creates a problem as communication is attempted over the RSU. In this study, high mobility and security problems are addressed through the use of consortium blockchain technology and wireless communication among vehicles. It is ensured that the blockchain is inherently secure and the speed problem is solved, avoiding the effect of high mobility. In addition, the proposed queue model helps prevent data loss during transaction processing.

According to the information provided in Table I, several blockchain-based studies from the literature and their comparison with the proposed system are presented.

The studies selected in Table I represent key contributions in their respective fields. As shown in Table I, the use of consortium-type blockchains is quite rare, similar to the proposed approach. As noted in the table, public blockchain are slow, making them less suitable for systems with high mobility. Private blockchains, on the other hand, carry risks in terms of security as they are managed by a single central authority. In addition, RSUs in most systems are very costly to use, as they add extra costs and security risks to the systems.

III. METHODOLOGY

In this section, the system architecture and technical details are mentioned. In this study, the messages transmitted to the consortium are kept in the queue structure to prevent them from being lost. During system evaluation, the performance of the implemented queue structure is compared with theoretical mathematical calculations. The closeness of the observed performance to the theoretically calculated values, along with achieving strong system performance by using the data integrity contribution of a technology such as

TABLE I. CONCEPTUAL COMPARISON OF THE PROPOSED MODEL WITH STUDIES IN THE LITERATURE

References	Blockchain Type	Mining Nodes	Consensus Mechanism	Negative Aspects According to the System
[29]	Public	Each node	PoW	It is quite slow as it uses a public blockchain and uses a PoW mechanism.
[48]	Consortium	RSUs	PBFT	It is also costly to implement due to the use of RSU.
[49]	Public	Each node	PoW	It is quite slow as it uses a public blockchain and uses a PoW mechanism.
[50]	Public	RSUs	Distributed consensus	It is quite slow as it uses a public blockchain. It is also costly to implement due to the use of RSU.
[51]	Public	RSUs	PoW	It is quite slow as it uses a public blockchain and uses a PoW mechanism
[52]	Public	Vehicle leader	PoW	It is quite slow as it uses a public blockchain and uses a PoW mechanism.
[53]	Private	RSUs	PoA	Since the decision mechanism of the system depends on a single place, it is problematic in terms of security. It is also costly to implement due to the use of RSU.
[54]	Public	RSUs	PoW	It is quite slow as it uses a public blockchain and uses a PoW mechanism.
[55]	Private	CA	PoW	Since the decision mechanism of the system depends on a single place, it is problematic in terms of security. Also, PoW is a rather slow consensus.
Proposed Work	Consortium	Each consortium nodes	PoA	Each consortium node takes part in the decision mechanism and it is sufficient for more than half of the nodes to approve. This is advantageous in terms of speed and security.

PBFT, practical byzantine fault tolerance; PoW, proof of work; RSUs, roadside units.

blockchain, which is not normally used in high mobility, constitutes an important contribution.

The primary limitation of the proposed system requirement for vehicles to have an active internet connection. Since RSUs are not utilized, all processes such as positioning verification and message exchange are performed directly through the internet connection between vehicles. Vehicles use wireless technologies to communicate among themselves. Joining the other system and verifying messages is done via an internet connection. Therefore, internet connectivity is a prerequisite for system operation. In this study, the proposed model is explained using case diagrams and pseudocodes. The most commonly used consortiums are blockchain and the PoA consensus algorithm. Details on how these general methods are interpreted are contained in the diagrams and pseudocodes. The contribution of the study here is that it shows a performance that coincides with mathematically calculated fast performance times. At the same time, the most important innovation is that by using the consortium blockchain with a pool structure, both reducing the system load and preventing data loss that may arise from system density.

To summarize the overall structure, as shown in Fig. 1, vehicles with internet connectivity can join the system and perform verification through the consortium pool. The consortium pool distributes transactions to authorized nodes using a queue-based mechanism. In the proposed architecture, a queue-based transaction management system is integrated into the PoA consensus process. When multiple vehicles simultaneously submit transaction requests to the network, these requests are temporarily stored in a transaction queue. Authorized validator nodes process transactions sequentially from this queue based on predefined priority rules and timestamp ordering. This mechanism helps prevent network congestion, reduces the likelihood of transaction collisions, and ensures reliable transaction validation even under high communication loads. As a result, the system maintains stable throughput and minimizes transaction delays in highly dynamic vehicular environments.

In this study, the messages transmitted to the consortium are stored in the queue structure to prevent data loss. During system evaluation, the extent to which the implemented queue structure aligns with theoretical mathematical calculations is analyzed. The proximity of the observed performance to theoretically calculated values and providing good performance by using the data integrity contribution of a technology such as blockchain, which is not normally used in high mobility, constitutes an important contribution. As shown in Fig. 2, the overall system design includes nodes, consortium structures, and vehicles. The figure illustrates that consortium nodes are used within the system. Vehicles can send their messages or requests to join the system to the consortium pool via the node closest to them. In this system, tests were performed for 5, 7, 9, and 11 nodes. These test results are presented in the results section.

General system pseudocode consists of the of the following methods:

main()
create vehicle for new
verify vehicle for communication
create block for communicated vehicle

In addition, the consortium nodes mentioned here, for example, can be thought of as static servers placed in certain points of a city with coverage in mind. It is assumed that these servers and vehicles have an internet connection. They communicate over an internet connection. Considering that the internet connection is faster and the probability of interruption is low, it is ensured that it communicates through the consortium node, which is close to the vehicle in terms

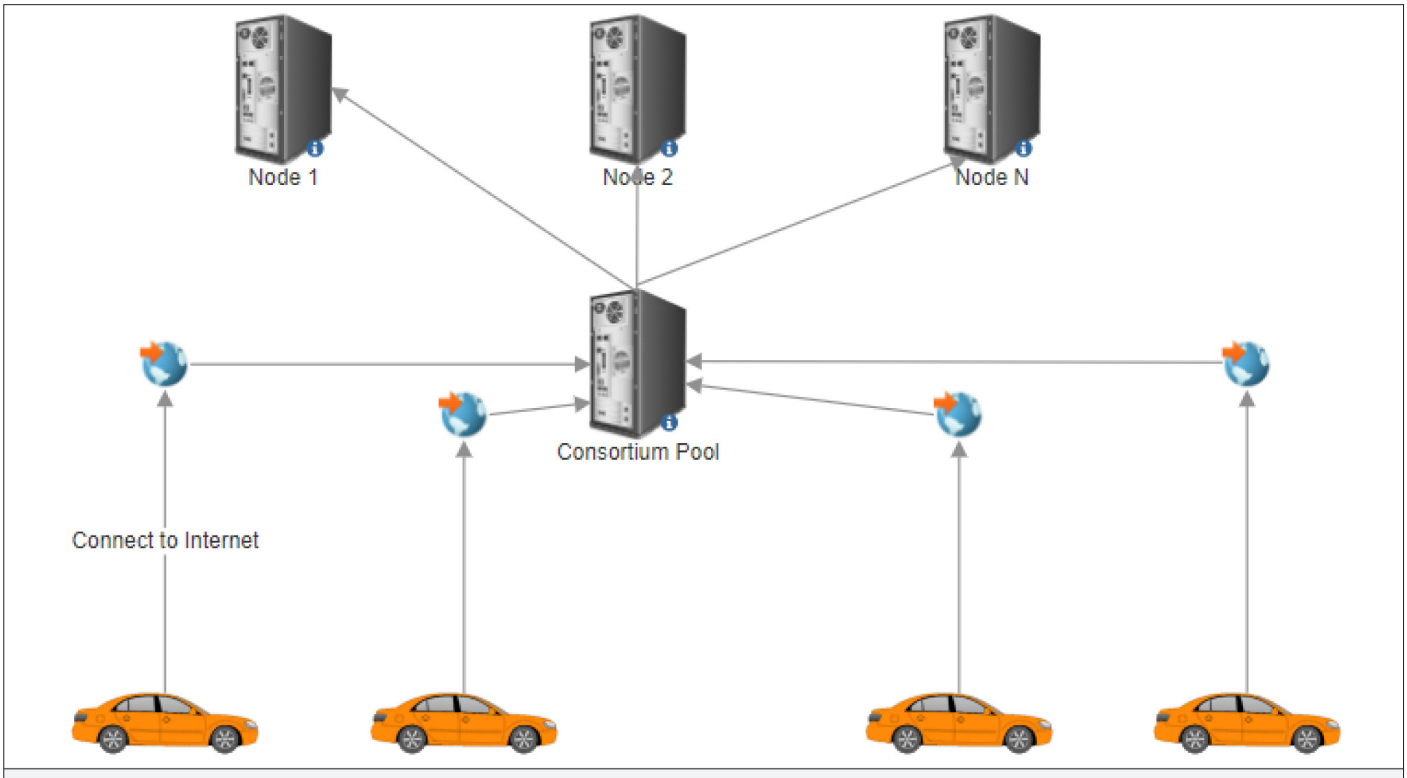

Figure 1. System structure

of location. In this system, it is located on a machine with a consortium pool. Considering that it is made for a city, the requests coming to the pool are sent sequentially to the nodes in the city.

As shown in Fig. 3, a vehicle sends a request to join the system through the nearest consortium node to join the system. As a result of the relevant request, public and private keys of the vehicle are generated. The generated keys are shared with the vehicle. The key information generated for the vehicle included in the system is shared with other consortium nodes.
The pseudocode of the algorithm used to be included in the system consists of the following methods.

createVehicle(vehicle)
find nearest node using vehicle's latitude and vehicle's longitude
send system enroll request for vehicle

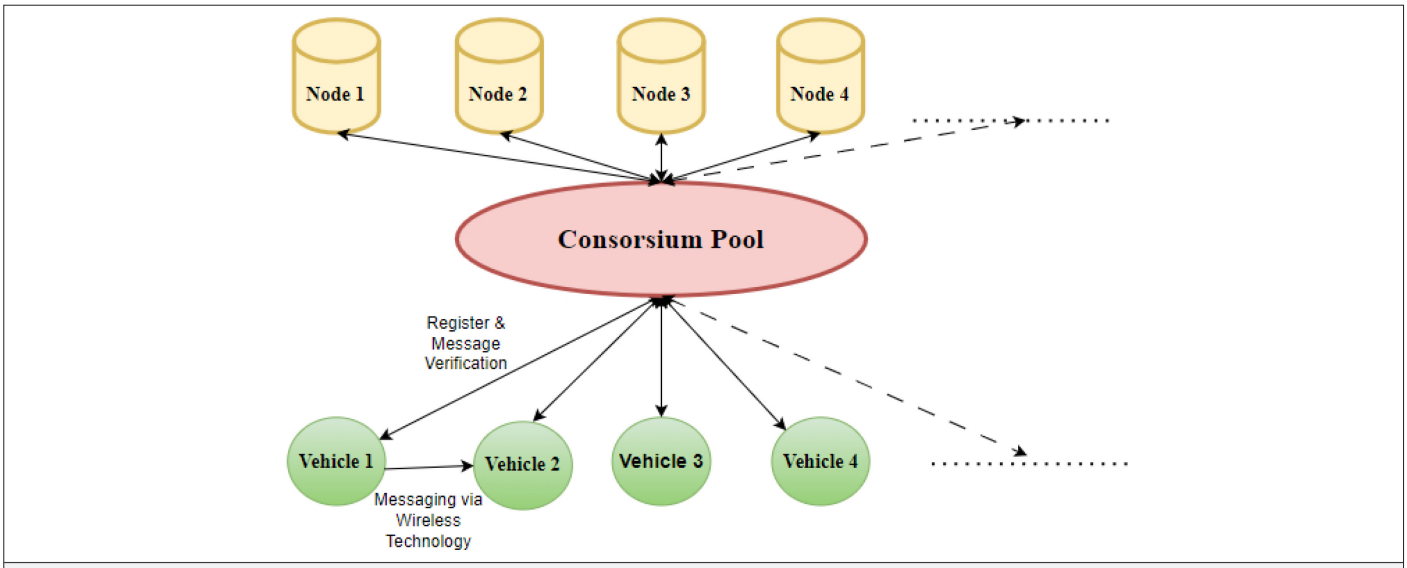

Figure 2. General system design

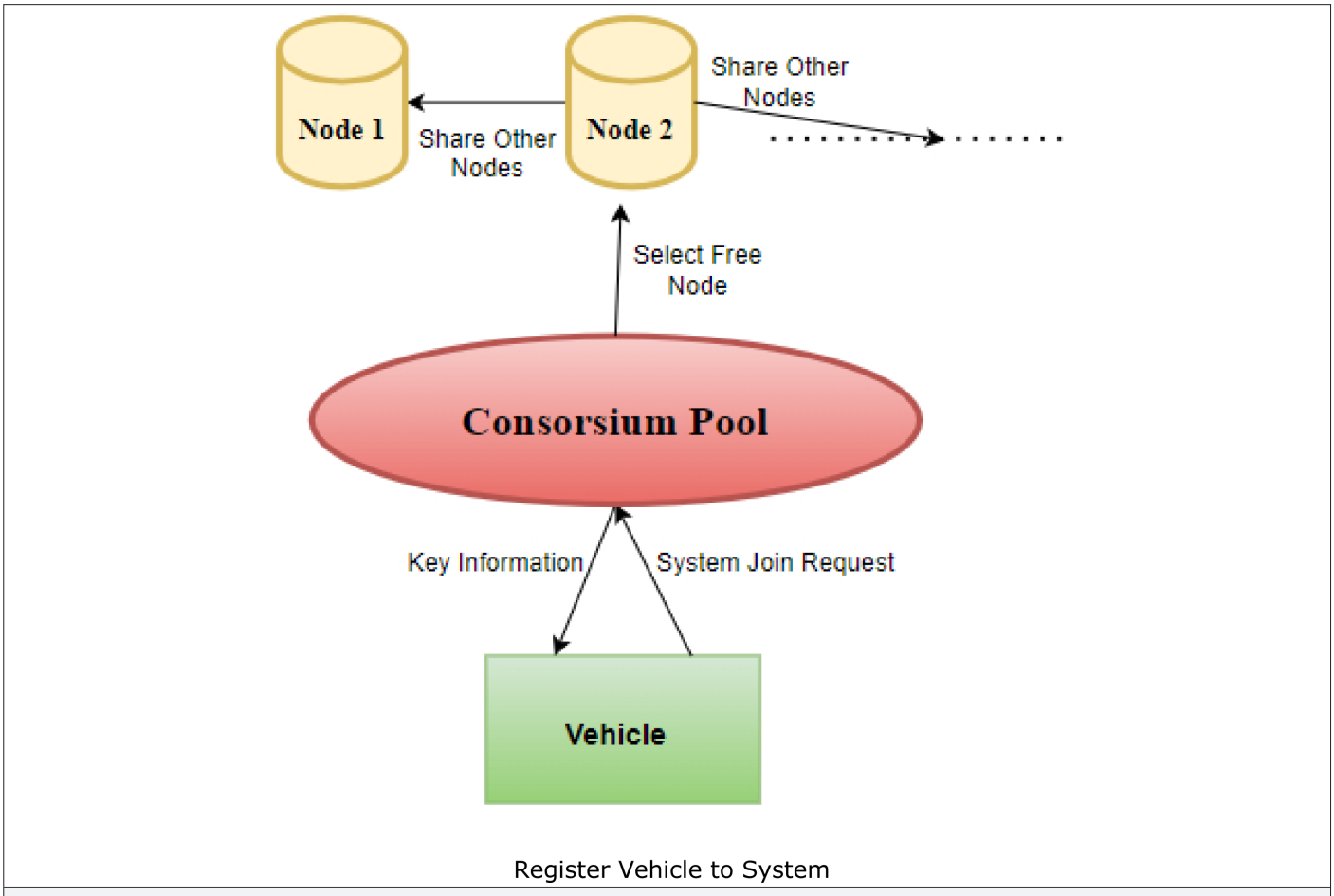

Figure 3. Register vehicle to system

With the above pseudocode, a vehicle that intends to join the system sends a request to the consortium pool and initiates the joining process through an available (idle) node.

sendSystemEnrollRequest(vehicle)
Generate PublicKey
Generate PrivateKey
Calculate Hash SHA256(vehicle, publicKey)
Add hash to address list map
Share Other Consortium Nodes

With the request to be included in the system created using the pseudo-code above, the public key, private key, and hash are created for the vehicle that creates the request. The generated hash is then added to the address list.

The key generation algorithm proceeds in the following order with mathematical formulas:

- Two large prime numbers are chosen, p and q,
- n value is calculated using p and q, $n = pq$
- ϕ is calculated, $\phi(n) = (p-1)(q-1)$
- A common prime value e between 1 and ϕ is selected, $e, 1 < e < \phi(n)$
- d is calculated by performing mode operation with ϕ, $de = 1(mod\ \phi(n))$
- Public Key is created using n and e (n,e),
- Private Key is created using n and d (n,d).

As shown in Fig. 4, a vehicle sends a message to another vehicle. To verify the transmitted message, the request to the consortium pool is shared with one of the idle consortium nodes. The verification result, whether approved or rejected by the selected node, is then returned to the requesting vehicle. Due to the use of PoA, which accelerates the system, there is no requirement for a 51% confirmation consensus as in classical blockchain. Instead, approval from a single consortium node, selected by the consortium pool, is sufficient. Additionally, the use of a queue mechanism helps prevent data loss. If verification fails, an error message is displayed; if verification is successful, the information is shared with other consortium nodes to be added to the blockchain. The integrity of the data is ensured by sharing it with other nodes. Since data integrity is the most important security element in the system, its security is ensured in this way.

createBlock(node, message)
verify node using message
add block to BlockChain

As shown in the code snippet above, the message information is sent to a node specified in the consortium pool. If the sent message is verified, it is added to the chain. Otherwise, an error message is displayed.

verify(message)
check AdresList for senderHash

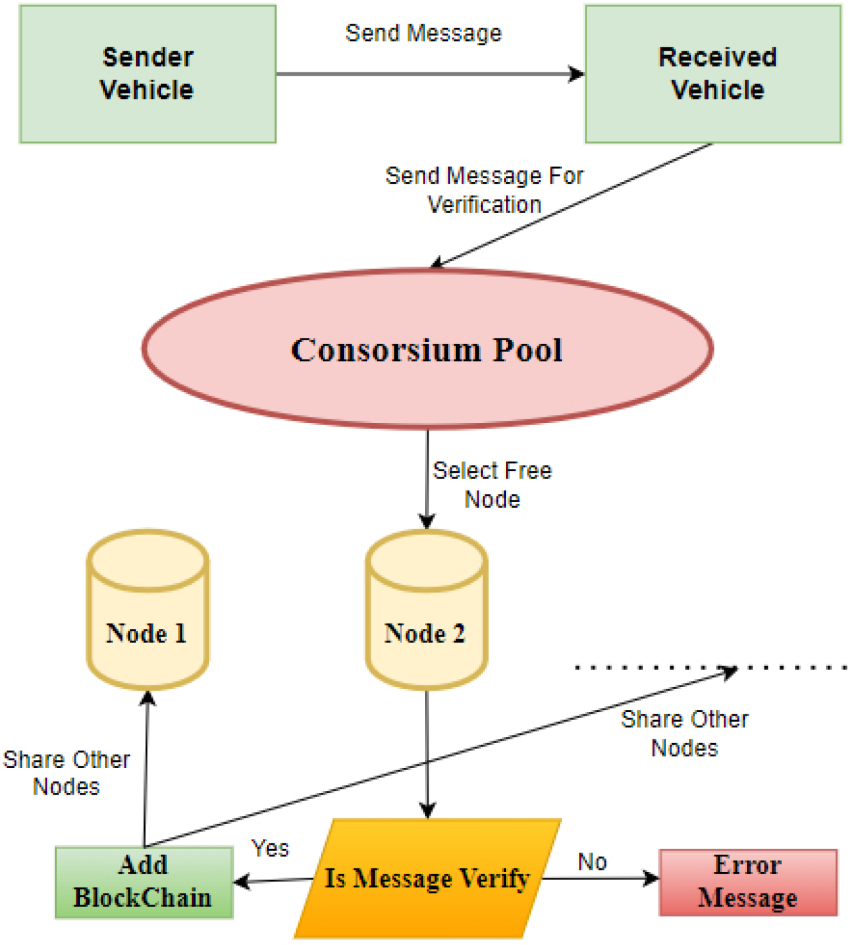

Figure 4. Message process

calculatedMerkleRoot using vehicle message
check calculatedMerkleRoot
calculate hash SHA256 using previousHash, calculatedMerkleRoot , timestamp
check calculatedHashCheck

In the pseudo-code above, the verification process is performed. During the verification process, it is first checked whether the vehicle that sent the message is included in the address list. If the address is not in the address list, an unknown vehicle error is issued.

Next, Merkle root is calculated and compared with the Merkle root value of the chain. If the calculated value does not match, an invalid root error is issued. Finally, the hash value is calculated and the accuracy of the calculated hash value is checked. If not correct, an invalid hash error is issued.

The steps in the messaging process in the system are as follows:

- A vehicle sends a message to another vehicle.
- The sender submits a verification request to the consortium pool.
- The message is forwarded to the consortium pool.
- The message is then assigned to a consortium node based on availability.
- The transaction received by the node is placed into a queue.
- If the message is verified, the confirmation response is returned.
- If the message is verified, it is added to the blockchain.
- The block information added to the chain is then shared with other consortium nodes

The node whose verification is requested makes a verification request to the consortium pool in the system. If verification occurs, the message is added to the chain. During the verification process, it is first checked whether the vehicle sending the message is included in the address list. If the address is not in the address list, an unknown vehicle error is issued.

The merkleRoot is then calculated, and it is checked whether the calculated value is the merkleRoot value of the chain. If the calculated value does not match, an invalid root error is thrown. Finally, the hash value is calculated and the accuracy of the calculated, hash value is checked.

The message that passes all the above-mentioned checks is added to the chain.

Based on the calculated complexity values, the process of adding a new vehicle to the system has a time complexity of O(1), whereas the messaging process has a complexity of O(log n). These results

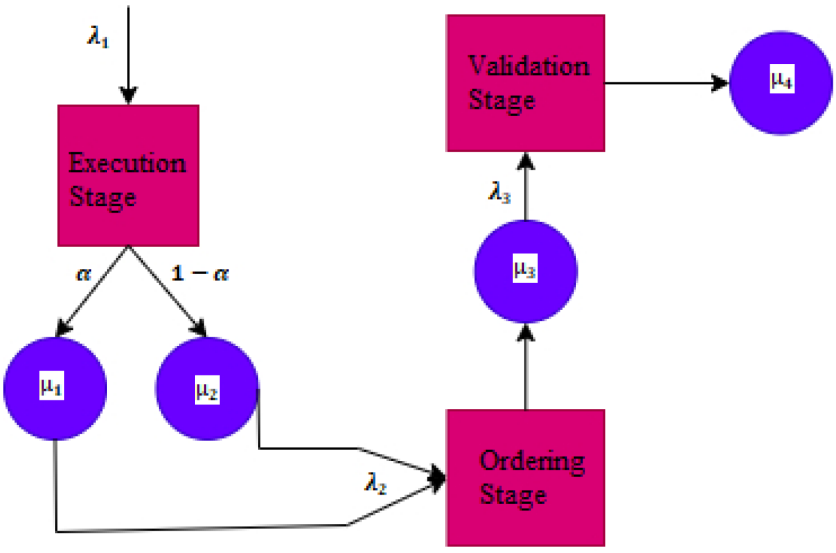

Figure 5. Queue model example

indicate strong performance for a high-mobility environment. A key contribution of the proposed design is that it effectively addresses the trade-off between speed and security by achieving both efficient processing and data integrity simultaneously.

The message that passes all the required checks proceeds through three main stages: execution, ordering, and verification (Fig. 5). These are the stages it goes through before being queued to reach the consortium node in the execution phase. The ordering stage is the stage in which the order is placed before the verification process. This stage is the last point of the section where the consortium pool is located. The verification phase is the stage where the decision is made as to whether or not it will be included in the chain at the node where it is processed.

In consortium-type blockchains, transactions are implemented in a queue network. There are some suggestions to make transactions more efficient in this queue network. The processes are divided into 3 stages. These are execution, ordering, and validation. The performance value for each of these stages is defined as transaction per second (TPS) and transaction latency. For example, let R be a random number. Let E be the expectation function. In this case, the mean response time at a random time is called E[R]. E[R] includes all 3 stages. These stages are named E[Re], E[Ro], and E[Rv]. TPS is calculated in (1). N_{trx} and T_p values are used when calculating TPS. N_{trx} value represents the number of transactions and T_p represents the transaction time. In (2), the mean response time is calculated. The N value in the related formula represents the number of members in the consortium, and E[N] represents its probabilistic value. Finally, the λ value is defined as the transaction arrival rate.

The first 5 equations show the formulation of the queuing model used in the proposed application [56]. The sum of the number of transactions calculated across each stage determines the value of E[N].

Equation 1 calculates TPS.

$$TPS = N_{trx} / T_p \tag{1}$$

This expression is included in (2). Equations 3, 4, and 5 present the calculation of E[Ne], E[No], and E[Nv], respectively. Here, Ne = Execution stage of N, No = Ordered stage of N, Nv = Validation stage of N, N = number of members, λ = transaction arrival rate, μ = average service time, $\tau_{e,v}$ is Neuts' rate matrix [57]):

$$E[N] = E[N_e] + E[N_o] + E[N_v] \tag{2}$$

$$E[N_e] = \pi_e \left(I - \tau_e\right)^{-2} . 1_e \tag{3}$$

$$E[N_o] = \lambda_2 / \left(\mu_3 - \lambda_2\right) \tag{4}$$

$$E[N_v] = \pi_v \left(I - \tau_v\right)^{-2} . 1_v \tag{5}$$

Equations 3, 4, and 5 express the mathematical statistical equivalent of each stage. In Equation 2, the sum of statistical values of each stage is considered. The corresponding values of the elements in (3), (4), and (5) above are given in the equations below. As an example, some examples show the execution stage.

$$\tau_{e,v} = \lambda\left(\lambda I - S_{e,v} - \lambda 1_{e,v} \beta_{e,v}\right)^{-1} \tag{6}$$

$$\beta_{e,v} = \left[\alpha 1 - \alpha\right] \tag{7}$$

$$S_{e,v} = \begin{bmatrix} -\mu_1 & 0 \\ 0 & -\mu_2 \end{bmatrix} \tag{8}$$

$$1_{e,v} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{9}$$

λ and μ values in the above equations are given in Fig. 5.

The calculated values are derived using the equations presented above. As shown in the results section, timer mechanisms in the software were used during computation of the test result. When using these mechanisms, the waiting time is calculated by using the difference between the time a message is queued and the time it is

TABLE IV. SYMBOLS AND EXPRESSIONS

Symbols or Expressions	Meaning
p and q	Large prime numbers
ϕ	$\phi(n) = (p-1)(q-1)$
N_{trx}	value represents the number of transactions
T_p	the transaction time
N	number of members
$[N_e],[N_o],[N_v]$	Execution stage of N, Ordered stage of N, Nv Validation stage of N
λ	transaction arrival rate
μ	average service time
$\tau_{e,v}$	Neuts' rate matrix [54]

processed from the queue and added to the chain. While performing this process, the IDs of the incoming messages, their arrival time, and the completion time of their processing are taken into account and produced as a software log. In these logs, each line contains the message ID, the time the relevant message arrived, the time the relevant message was completed, the waiting time of the relevant message, and the average waiting time of the messages received so far at Table IV.

IV. RESULTS

This section presents the results obtained using the defined performance metrics, along with comparative tables. Since most related studies do not provide direct algorithm implementations or detailed performance timing information, a direct comparison with existing work is generally not possible. However, the performance times presented in the figures indicate efficient processing suitable for high-mobility vehicular environments. These times are first derived mathematically and then validated through experimental testing and measurement.

The proposed model follows the logic mentioned in the previous sections. The data used in communication between vehicles is produced synthetically and used for testing purposes. The system network being used is shown in Fig. 6. In total, there are nodes for the consortium and a certificate for validation at each node. An ordering mechanism is established between these nodes. Each node is installed on one computer as a Docker container. This process was carried out with virtualization on a computer. In other words, although each node is physically on the same machine, they are virtual devices with separate addresses. The blockchain algorithm, which is given the pseudocodes mentioned in the previous section, is installed on each node.

Additionally, this study compares the time spent by the synthetically generated messages in the system with the data obtained from mathematical calculations to evaluate the efficiency of the algorithm and its alignment with theoretically calculated performance values. The experiments were conducted using 100 simultaneous messages.

The physical machine used has an Intel(R) Core(TM) i5-5200U CPU (2.2 GHz) with 8 GB DDR4 RAM. The operating system is Windows 10 64-bit operating system. The duration of each process is obtained by printing the processing times in the logged records of each stage. Statistical, conceptual, and test results are examined over these periods.

The performance evaluation of the proposed blockchain-based V2V communication model was conducted using a simulation-based analysis combined with mathematical queue theory. The simulation environment was designed to represent a vehicular communication scenario where multiple vehicles generate transaction requests simultaneously.

In the simulation model, vehicles act as nodes that generate and transmit communication messages through a consortium blockchain

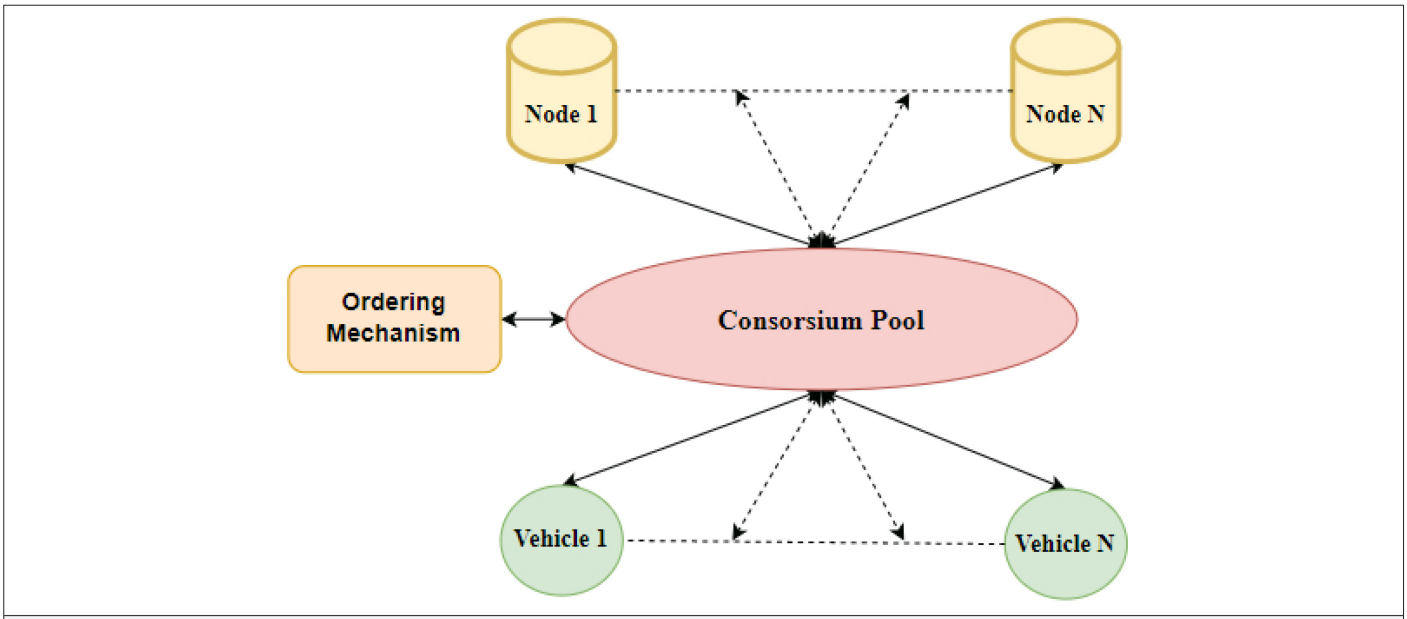

Figure 6. System network topology

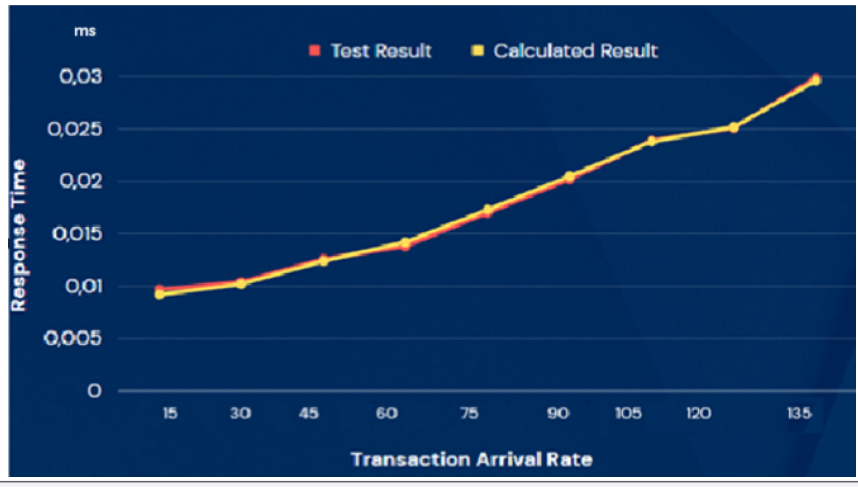

Figure 7. Execution stage testing and calculated value

network using the PoA consensus mechanism. Transactions generated by vehicles are temporarily stored in a queue structure before being validated by authorized validator nodes.

As an example, the calculated values and the test values whose graphs are given are for 11 consortium nodes. According to the proposed algorithm, increasing the number of nodes up to 11 gives positive results. Therefore, the graphs presented focus on 11 nodes, which yielded the best performance in the experiments. Naturally, the calculated values will vary with different numbers of nodes, so graphs are provided based on the specific node counts tested. Additionally, due to the characteristics of the algorithm, performance is expected to improve as the number of nodes increases, since waiting time decreases with a larger number of consortium nodes. The results for 11 nodes are presented because this number represents the maximum capacity that could be supported by the physical machine used in the experiments.

The calculated and tested times are calculated as stated in the findings section for the execution phase. The graph in Fig. 7 is obtained using transaction arrival rate and average response time. When the graph is examined, the results match the calculated value, except for the case when the transaction arrival rate is less than 20. The reason for the lack of overlap is that the rate is low and the graph is at the level of ten thousandths. With these calculations, the efficiency of the system is over 90%.

The calculated and tested times are calculated as stated in the findings section for the ranking stage. The graph in Fig. 8 is obtained using transaction arrival rate and average response time. When the graph is examined, the results match the calculated value, except for the case where the transaction arrival rate is between 20 and 40. The reason for the lack of overlap is that the rate is low and the graph is at the level of ten thousandths. Deviation is also acceptable in non-overlapping cases. With these calculations, the efficiency of the system is over 95%.

The calculated and tested times are calculated as stated in the findings section for the verification phase. The graph in Fig. 9 is obtained using transaction arrival rate and average response time. Additionally, as can be seen in the same figure, the number of transaction arrival rates does not exactly coincide with 20 and 40. The reason for this is that the rate is low and the graph is at the level of one in ten thousand. The amount of non-overlap in the relevant data is also acceptable. The efficiency of the system is over 90%.

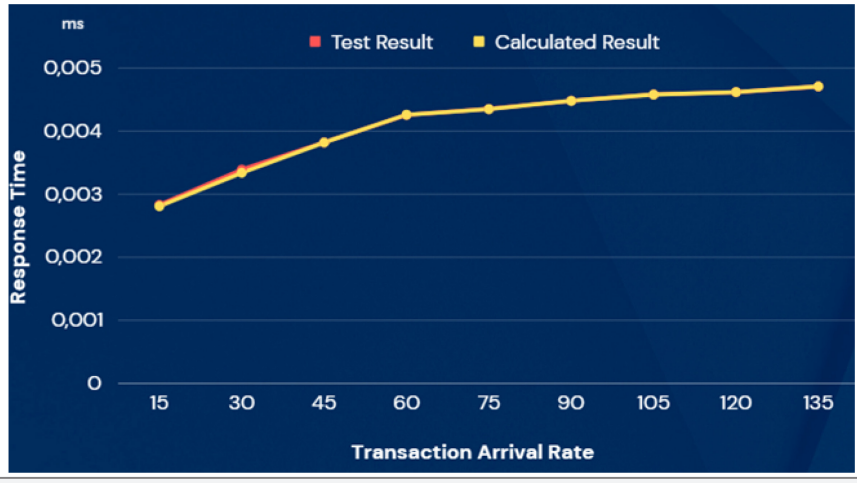

Figure 8. Ordering stage test and calculated value

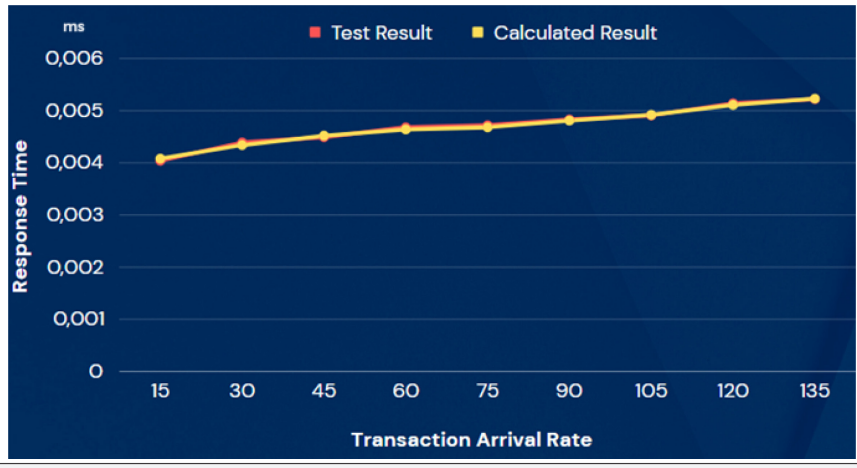

Figure 9. Validation stage test and calculated value

TABLE II. PERFORMANCE COMPARISON BETWEEN THE PROPOSED BLOCKCHAIN–BASED V2V MODEL AND EXISTING ARCHITECTURES IN THE LITERATURE

Ref	Blockchain Type	Queue Structure	Consensus Algorithm	Average Time (Milliseconds)
[58]	Public	No	Unknown	221
[59]	Private	No	PoS	125.08
[60]	Private	Yes	Raft	39.585
[61]	Private	No	PoW	41.083
Proposed work	Consortium	Yes	PoA	14.98

The studies selected in Table I are the most important in their field. As shown in Table II, the use of consortium-type blockchains is quite rare, as in the study. As mentioned in the table, since the general blockchain is a slow system, it is not suitable for systems with high mobility. Private blockchains, on the other hand, carry security risks because they are managed by a single central authority. Additionally, the use of RSUs in most systems is very costly as it adds extra costs and security risks to the systems.

As shown in Table II, the types of blockchain used in the compared studies vary. At the same time, the structures established and the logic of adding them to the chain also differ. However, the system seems to be in a good place in terms of the average time given by the generally used system. The factors taken into consideration in the compared studies are the blockchain type, whether the queue structure is used in the proposed models, and the consensus algorithm. Especially the blockchain type and consensus algorithm are factors that directly affect the speed. Although the existence of a queue structure affects the transaction waiting time, it is an important factor that reduces data loss.

The transaction arrival rate of the test process used for this study is 70, which is applied uniformly across all stages. Additionally, the number of simultaneously processed messages is set to 100. As noted previously, increasing the number of nodes in the algorithm mproves performance; therefore, the results of the 5-node consortium are included in the comparison table. Five nodes were selected because this represents the minimum number of nodes from which sample results could be obtained.

The system performs efficiently regardless of the number of nodes. However, analysis of the test results shows that, with a constant message traffic, increasing the number of nodes improves system performance, resulting in reduced average waiting times. Table III presents values based on transaction arrival rate and number of nodes. In this study, the test transaction arrival rate is set to 70.

V. CONCLUSIONS

This study presents an effort to develop a secure model using blockchain for inter-vehicle communication. The most important paradox in this study, from the very beginning, is the dilemma of performance and security. It is difficult to provide both security and fast communication in a high-mobility environment, such as vehicle communication. To overcome this, data security is ensured through the use of public and private key infrastructure provided

TABLE III. PERFORMANCE COMPARISONS PROPOSED MODEL NUMBER OF CONSORTIUM NODE

Number of Node	Execution Stage (Average) (Milliseconds)	Ordering Stage (Average) (Milliseconds)	Validation Stage (Average) (Milliseconds)	Total Average Waiting Time (Milliseconds)
5	3.6	8.6	2.78	14.98
7	3.52	8.51	2.65	14.68
9	3.45	8.38	2.58	14.41
11	3.34	8.25	2.46	14.05

by blockchain technology. To increase the speed of these transactions, it is preferred to use a consortium blockchain. Consortium blockchain is considered a suitable approach for high-mobility environments due to its balance between security and performance. In addition, the PoA consensus algorithm is employed to eliminate the traditional requirement of obtaining more than 50% approval for ledger registration, thereby reducing processing delays. In this way, there is no additional waiting time for system inclusion. In order not to lose incoming requests, that is, to avoid data loss, a consortium pool is created before all consortium nodes, and a queue structure is created in the relevant pool. The performance analysis of the proposed queue structure has been examined, and comparisons have been made with related studies. Based on the overall results, the system is observed to achieve performance levels aligned with the mathematically derived targets and to perform strongly compared to existing studies.

This study is carried out by comparing the theoretically calculated values with the values on which the system is tested. The major limitation of this project is the lack of access to source code or comparable elements of previous work. For this reason, the results of the study are compared with their theoretical values.

In summary, the proposed model employs a consortium blockchain along with the PoA consensus algorithm to protect data integrity in inter-vehicle communication while also considering the speed of a highly mobile system. The experimental results conducted to validate the mathematical performance show a strong agreement with the theoretically calculated values, as reflected in the tables. In addition, the results indicate that system performance improves as the number of consortium nodes increases.

In future work, an additional security metric with a mathematical foundation is intended to be incorporated into the performance evaluation criteria. The proposed security criteria will also be assessed under various attack scenarios. Furthermore, the number of consortium nodes and the queue-based model will be re-evaluated to explore potential improvements in system performance.

Data Availability Statement: The data that support the findings of this study are available on request from the corresponding author.

Artificial Intelligence Usage Statement: The authors declared that no artificial intelligence tool was used in the preparation of the manuscript.

Peer-review: Externally peer-reviewed.

Author Contributions: Concept – S.O., F.K.; Design – S.O.; Supervision – S.O., F.K.; Resources – S.O.; Materials – S.O.; Data Collection and/or Processing – S.O.; Analysis and/or Interpretation – S.O.; Literature Search – S.O., F.K.; Writing – S.O.; Critical Review – S.O., F.K.

Declaration of Interests: The authors have no conflict of interest to declare.

Funding: The authors declared that this study has received no financial support.

REFERENCES

1. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, 2017. [CrossRef].
2. K. P. Huang, S. Lo, and D. Sutthiphisal, "From data transparency and security to interfirm collaboration-A blockchain technology perspective," *ABAC J.*, vol. 43, no. 3, pp. 12–25, 2023. [CrossRef].
3. Ş. Okul, F. Keleş, and M. A. Aydin, "Vehicular social network using blockchain technology," *Istanb. Sabahattin Zaim Univ. J. Inst. Sci. Techmology*, vol. 4, no. 3, pp. 138–141, 2023. [CrossRef].
4. M. S. Sheikh, J. Liang, and W. Wang, "A survey of security services, attacks, and applications for vehicular ad hoc networks (VANETs)," *Sensors (Basel)*, vol. 19, no. 16, 3589, 2019. [CrossRef].
5. M. Q. A. Kaan Yıldırım, and A. Boyacı, "A comparision of VANET routing protocol performance for emergency situation," *Istanb. Commer. Univ. J. Technol. Appl. Sci.*, vol. 1, no. 1, pp. 1–10, 2018.
6. I. Wahid et al., "Vehicular ad hoc networks routing strategies for intelligent transportation system," *Electronics*, vol. 11, no. 15, p. 2298, 2022. [CrossRef].
7. M. Takaoğlu, Ö. Z. E. R. Çağdaş, and E. Parlak, "Blockchain technology and possible implementation areas in Turkey," *Int. J. East. Anatolia Sci. Eng. Des.*, vol. 1, no. 2, pp. 260–295, 2019.
8. A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT Challenges and opportunities," *Future Gener. Comput. Syst.*, vol. 88, pp. 173–190, 2018. [CrossRef].
9. O. C. Uchani Gutierrez, and G. Xu, "Blockchain and smart contracts to secure property transactions in smart cities," *Appl. Sci.*, vol. 13, no. 1, p. 66, 2023. [CrossRef].
10. J. Moodley et al., "Beyond reality: An application of extended reality and blockchain in the metaverse." 2023 IEEE International Conference on Omni-layer Intelligent Systems (COINS), 2023, pp.1–4. [CrossRef].
11. S. Nakamoto, "*Internet: Bitcoin: A Peer-to-Peer Electron. Cash Syst.*", vol. 221, no. 9986. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1, [Accessed: 07.04.2024].
12. R. Beck, "Beyond bitcoin: The rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, 2018. [CrossRef].
13. B. A. Tama, B. J. Kweka, Y. Park, and K.-H. Rhee, "A critical review of blockchain and its current applications." 2017 International Conference on Electrical Engineering and Computer Science (ICECOS), 2017, pp. 109–113. [CrossRef].
14. H. Halpin, and M. Piekarska, "Introduction to security and privacy on the blockchain." 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2017. [CrossRef].
15. F. Hawlitschek, B. Notheisen, and T. Teubner, "The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy," *Electron. Commer. Res. Appl.*, vol. 29, pp. 50–63, 2018. [CrossRef].
16. J. Leng, M. Zhou, J. L. Zhao, Y. Huang, and Y. Bian, "Blockchain security: A survey of techniques and research directions," *IEEE Trans. Serv. Comput.*, vol. 15, no. 4, pp. 2490–2510, 2022. [CrossRef].
17. I. Nath, "Data exchange platform to fight insurance fraud on blockchain." 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW). New York: IEEE, 2016, pp. 821–825. [CrossRef].
18. A. Lewis, "*Internet: so, You Want Use Blockchain That*". Available: https://www.coindesk.com/want-use-blockchain/, [Accessed: 07.04.2024].
19. V. Buterin, *"Internet: On Public and Private Blockchains, Ethereum Blog Crypto Renaissance Salon."* Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.[Accessed:07.04.2024].
20. J. H. Khor, M. Sidorov, and S. A. B. Zulqarnain, "Scalable lightweight protocol for interoperable public blockchain-based supply chain ownership management," *Sensors (Basel)*, vol. 23, no. 7, 3433, 2023. [CrossRef].
21. Y. Wang, T. Che, X. Zhao, T. Zhou, K. Zhang, and X. Hu, "A blockchain-based privacy information security sharing scheme in industrial Internet of things," *Sensors (Basel)*, vol. 22, no. 9, 3426, 2022. [CrossRef].
22. T. M. Fernandez-Carames, and P. Fraga-Lamas, "A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories," *IEEE Access*, vol. 7, pp. 45201–45218, 2019. [CrossRef].
23. A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," In Proceedings of the 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), Pittsburgh, PA, USA, 18–21 April 2017: IEEE: New York, NY, USA, pp. 173–178. [CrossRef].
24. A. Rahman et al., "DistB-condo: Distributed blockchain-based IoT-SDN model for smart condominium," *IEEE Access*, vol. 8, pp. 209594–209609, 2020. [CrossRef].
25. C. Loklindt, M. P. Moeller, and A. Kinra, "How blockchain could be implemented for exchanging documentation in the shipping industry," In

International Conference on Dynamics in Logistics. Berlin/Heidelberg, Germany: Springer, 2018, pp. 194–198.
26. B. B. Gupta, Mamta, R. Mehla, W. Alhalabi, and H. Alsharif"", "Blockchain technology with its application in medical and healthcare systems: A survey," *Int. J. Intell. Syst.*, vol. 37, no. 11, pp. 9798–9832, 2022. [CrossRef].
27. A. F. M. S. Akhter, M. Ahmed, A. F. M. S. Shah, A. Anwar, and A. Zengin, "A secured privacy-preserving multi-level blockchain framework for cluster based VANET," *Sustainability*, vol. 13, no. 1, p. 400, 2021. [CrossRef].
28. C. Wang, J. Shen, J. F. Lai, and J. Liu, "B-TSCA: Blockchain assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs," *IEEE Trans. Emerg. Top. Comput.*, vol. 9, no. 3, pp. 1386–1396, 2021. [CrossRef].
29. R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 177–186, 2020. [CrossRef].
30. A. S. Kulathunge, and H. R. O. E. Dayarathna, "Communication framework for vehicular ad-hoc networks using Blockchain: Case study of Metro Manila Electric Shuttle automation project," In Proceedings of the 2019 International Research Conference on Smart Computing and Systems Engineering (SCSE), Colombo, Sri Lanka, 28 March 2019;. IEEE: New York, NY, USA, pp. 85–90. [CrossRef].
31. H. Taghizadeh, and V. Solouk, "A novel MAC protocol based on cooperative master-slave for V2V communication," In Proceedings of the 2015 38th International Conference on Telecommunications and Signal Processing (TSP), Prague, Czech Republic, 9–11 July 2015; IEEE: New York, NY, USA, pp. 1–5. [CrossRef].
32. C. Lai, and Y. Ding, "A secure blockchain-based group mobility management scheme in VANETs," In Proceedings of the 2019 IEEE/CIC International Conference on Communications in China (ICCC), Changchun, China, 11–13 August 2019; IEEE: New York, NY, USA, pp. 340–345. [CrossRef].
33. U. Javaid, M. N. Aman, and B. Sikdar, "DrivMan: Driving trust management and data sharing in VANETS with blockchain and smart contracts," In Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 28 April–1 May 2019; IEEE: New York, NY, USA, 2019, pp. 1–5. [CrossRef].
34. I. Ali, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *J. Syst. Archit.*, vol. 99, 101636, 2019. [CrossRef].
35. Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018. [CrossRef].
36. X. Zhang, and X. Chen, "Data security sharing and storage based on a consortium blockchain in a vehicular ad-hoc network," *IEEE Access*, vol. 7, pp. 58241–58254, 2019. [CrossRef].
37. N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," In *Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. New York, NY, USA: IEEE, 2018, pp. 674–679. [CrossRef].
38. C. Lin, D. He, X. Huang, N. Kumar, and K. K. R. Choo, "BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 12, pp. 7408–7420, 2021. [CrossRef].
39. C. Zhang, R. Lu, X. Lin, P. H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," In *Proceedings of the IEEE INFOCOM 2008-The 27th Conference*. New York: IEEE, 2008, pp. 246–250. [CrossRef].
40. J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, 2016. [CrossRef].
41. M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, 2017. [CrossRef].
42. H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu, "FADB: A fine-grained access control scheme for VANET data based on blockchain," *IEEE Access*, vol. 8, pp. 85190–85203, 2020. [CrossRef].
43. H. Luo et al., "ESIA: An efficient and stable identity authentication for Internet of vehicles," in *IEEE Trans. Veh. Technol.*, vol. 73, No. 4, pp. 5602–5615, 2024. [CrossRef].
44. X. Yang, H. Luo, J. Duan, and H. Yu, "Ultra reliable and low latency authentication scheme for Internet of vehicles based on blockchain." IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), New York, NY, USA, 2022, pp. 1–5. [CrossRef].
45. M. A. Khan, A. Rehman, and B. S. Kim, "Blockchain-based secure communication framework for Internet of Vehicles," *IEEE Access*, vol. 11, pp. 35421–35433, 2023.
46. Y. Wang, H. Zhang, and X. Li, "A lightweight blockchain architecture for scalable Internet of Vehicles communication systems," *Future Gener. Comput. Syst.*, vol. 145, pp. 112–123, 2024.
47. L. Zhou, J. Chen, and K. Xu, "Blockchain-enabled secure vehicle-to-vehicle communication in intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 7, pp. 7564–7575, 2023.
48. C. Chen, J. Wu, H. Lin, W. Chen, and Z. Zheng, "A secure and efficient blockchainbased data trading approach for Internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 68, no. 9, pp. 9110–9121, 2019. [CrossRef].
49. A. Mostafa, "A general framework for detecting malicious vehicles," *J. Commun.*, vol. 14, pp. 356–362, 2019.
50. A. S. Khan, K. Balan, Y. Javed, S. Tarmizi, and J. Abdullah, "Secure trust-based blockchain architecture to prevent attacks in VANET," *Sensors (Basel)*, vol. 19, no. 22, 4954, 2019. [CrossRef].
51. M. Baza et al., "Detecting sybil attacks using proofs of work and location in VANETs," *IEEE Trans. Depend. Sec. Comput.*, vol. 1, no. 1, p. 99, 2020.
52. M. Wagner, and B. McMillin, "Cyber-physical transactions: A method for securing VANETs with blockchains," in 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), IEEE. New York: IEEE, 2018, pp. 64–73. [CrossRef].
53. M. Li, J. Weng, A. Yang, J.-N. Liu, and X. Lin, "Toward blockchain-based fair and anonymous ad dissemination in vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11248–11259, 2019. [CrossRef].
54. D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019. [CrossRef].
55. A. Patel, N. Shah, T. Limbasiya, and D. Das Vehiclechain, "Blockchain-based vehicular data transmission scheme for smart city," in 2019 IEEE International Conference on Systems, Man and Cybernetics (SMC), IEEE, 2019, pp. 661–667.
56. A. H. Salem, A. Abdel-Hamid, and M. A. El-Nasr, "The case for dynamic key distribution for PKI-based VANETS," *Int. J. Comput. Netw. Commun.*, vol. 6, no. 1, pp. 67–78, 2014.
57. Internet. Available: https://web.mst.edu/~gosavia/queuing_formulas.pdf. [Accessed: 07.04.2024].
58. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "ProvChain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, Spain, 2017, pp. 468–477. [CrossRef].
59. S. Chen, J. Zhang, R. Shi, J. Yan, and Q. Ke, "A comparative testing on performance of blockchain and relational database: Foundation for applying smart technology into current business systems," In *Distributed, Ambient and Pervasive Interactions: Understanding Humans. DAPI 2018. Lecture Notes in Computer Science*, vol 10921, N. Streitz, and S. Konomi, Ed. Cham: Springer International Publishing, 2018, pp. 21–34. [CrossRef].
60. T. Yan, W. Chen, P. Zhao, Z. Li, A. Liu, and L. Zhao, "Handling conditional queries on Hyperledger Fabric efficiently," In *Web Inf. Syst. Eng. – WISE 2019. WISE 2020. Lecture Notes in Computer Science*, vol 11881, R. Cheng, N. Mamoulis, Y. Sun, and X. Huang, Eds., Cham, Switzerland: Springer, 2019, pp. 200–215.
61. A. Badr, L. Rafferty, Q. H. Mahmoud, K. Elgazzar, and P. C. K. Hung, "A permissioned blockchain-based system for verification of academic records," 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Canary Islands, Spain, 2019, pp. 1–5. [CrossRef].



Şükrü Okul is a Researcher at TÜBİTAK BİLGEM. He received his Ph.D. in Computer Engineering from Istanbul University Cerrahpaşa in 2024. He earned his M.Sc. in Computer Engineering from Istanbul University between 2016 and 2018, with his thesis focusing on "Security Attacks Analysis for Smart Cars." He completed his B.Sc. in Computer Science and Engineering at Marmara University from 2009 to 2014. Turkish is his native language, and he is fluent in English.



Fatih Keleş received his B.Sc. degree in Electronics and Communication Engineering from Yıldız Technical University, Istanbul, in 2000. He earned his M.Sc. degree in Electronics Engineering from Yıldız Technical University, Istanbul, in 2003 and his Ph.D. degree in Electronics Engineering from the same institution in 2010. He joined the Computer Engineering Department of Yıldız Technical University in 2001 and is currently an Assistant Professor in the Computer Hardware and Embedded Systems Division of the Computer Engineering Department at Istanbul University-Cerrahpaşa, Istanbul. Dr. Keleş continues to teach both compulsory and optional hardware courses at the undergraduate and graduate levels. His research interests include neural networks, circuit theory, microprogramming and control structures, embedded systems, robotics, pattern recognition, semiconductor materials, analog circuit design, and hardware implementations of neural networks.