Thesis for the Degree of Bachelor of Science in Computer Science and Engineering

Blockchain based Message Dissemination in Vehicular Ad Hoc Networks

Sidratul Muntaha - 180041118

Ramisa Maliat - 180041131

Urbana Musharrat Haider - 180041110

Department of Computer Science and Engineering
Islamic University of Technology
Gazipur, Bangladesh

May, 2023

Blockchain based Message Dissemination in Vehicular Ad Hoc Networks

Sidratul Muntaha - 180041118

Ramisa Maliat - 180041131

Urbana Musharrat Haider - 180041110

Department of Computer Science and Engineering
Islamic University of Technology
Gazipur, Bangladesh

May, 2023

Blockchain based Message Dissemination in Vehicular Ad Hoc Networks

Authors

Sidratul Muntaha - 180041118

Ramisa Maliat - 180041131

Urbana Musharrat Haider - 180041110

Supervised by

Dr. Muhammad Mahbub Alam

Professor

Department of Computer Science and Engineering

Islamic University of Technology

Co-supervised by

S. M. Sabit Bananee

Lecturer

Department of Computer Science and Engineering

Islamic University of Technology

Submitted to
the Department of Computer Science and Engineering of
Islamic University of Technology
as a requirement for the degree of
Bachelor of Science in Computer Science and Engineering

Declaration Of Authorship

We hereby confirm that the research and simulations are conducted by **Sidratul Muntaha**, **Ramisa Maliat** and **Urbana Musharrat Haider** under the guidance of **Prof. Dr. Muhammad Mahbub Alam** and **S. M. Sabit Bananee, Lecturer** from the Department of Computer Science and Engineering (CSE) at the Islamic University of Technology (IUT), Gazipur, Bangladesh. We affirm that this thesis and its contents have not been submitted elsewhere for any academic degree or diploma. Proper attribution has been provided for information obtained from published and unpublished works of others, as evidenced by the citations and reference list included in the text.

Authors:

Sidratul Muntaha, Student ID- 180041118

Ramisa Maliat, Student ID- 180041131

Urbana Musharrat Haider, Student ID- 180041110

Supervisor:

Dr. Muhammad Mahbub Alam
Professor
Department of Computer Science and Engineering
Islamic University of Technology (IUT)

Co-supervisor:

S. M. Sabit Bananee
Lecturer
Department of Computer Science and Engineering
Islamic University of Technology (IUT)

Abstract

Vehicular Adhoc Networks (VANETs) is a promising research interest in the field of wireless networks. It is an application of the principle of Mobile Adhoc Networks (MANETs). It is used to provide services such as road safety, navigation, traffic monitoring etc. The continuously changing topology of the network introduces challenges in implementing VANET. Resolving these challenges following different strategies introduces other trade-offs. One of the most important applications in VANET is to disseminate incident messages to nearby vehicles. The effectiveness of the application depends on the correctness of the incident message and its timely delivery to the vehicles. Blockchain is one of the mechanisms that can be used in this respect. Consensus mechanism is used to validate the message and then a proper forwarding mechanism is used to disseminate the message. An incentive mechanism is used to encourage honest behaviour of the nodes.

The prominent consensus mechanisms used in blockchain such as Proof of Work (PoW), Proof of Stake (PoS), Proof of Elapsed Time (PoET) are not suitable to be used in VANET in their basic form. For example, PoW is highly time consuming and PoS is biased. Among the existing ones Practical Byzantine Fault Tolerant (PBFT) is the most suitable one for blockchain based VANET. So in our thesis we propose a new consensus mechanism which is a hybrid of the best practices of PoW and PBFT. It includes selective voting mechanism with weighted values for faster and more accurate validation. The threshold values are updated whenever needed. Limiting the number of voters makes the entire process efficient. The challenges in this respect are handled by imposing proper conditions on the voters. The concept of weighted sum of votes is introduced where honest voters are prioritized over others which results in higher accuracy in message validation in shorter amount of time.

Efficient selection of relay nodes ensures minimum latency in the dissemination process by ensuring minimum number of messages are passed. It also ensures quality of the message being passed. Along with the consensus mechanism we also present a mechanism to select relay nodes which will give the best performance in the message dissemination process by selecting node that will cover the maximum possible distance. The selected nodes spread the message to the maximum number of vehicles with the minimum number of broadcast messages. The

forwarding process is continued until a threshold is reached.

An incentive mechanism based on both reputation and monetary units is also proposed which will encourage integrity and honest behaviour from the vehicles. Previous works show the success of incentive mechanism based on both reputation and monetary units over the ones based on only one of them. We also integrate the concept of reputation in the validation process to increase its importance.

The simulation is done in the Omnet++ simulator platform integrated with Sumo. We showed the analysis of the results obtained from the simulation. The results give impressive improvements from the existing systems.

Acknowledgment

We wish to express our utmost appreciation for the divine favors bestowed upon us by the Almighty Allah, which have played a vital role in shaping this research. The successful completion of this thesis would not have been feasible without the steadfast backing, motivation, and guidance provided by numerous individuals, to whom we extend our sincere gratitude.

Our Supervisor, **Prof. Dr. Muhammad Mahbub Alam**, from the Department of Computer Science and Engineering at the Islamic University of Technology (IUT), deserves our deepest gratitude. His invaluable guidance, extensive expertise, and unwavering assistance have been pivotal in our journey.

We would also like to convey our thanks to our Co-supervisor, **S.M. Sabit Bananee**, a Lecturer from the Department of Computer Science and Engineering at the Islamic University of Technology (IUT). His perceptive deliberations, precious counsel, constant passion, and words of encouragement have played a decisive role in our work and significantly contributed to our achievements.

Lastly, we would like to express our profound appreciation to our cherished parents and siblings. Their limitless affection, unwavering support, and profound spiritual and emotional fortitude have served as unwavering wellsprings of inspiration throughout our academic endeavors.

Table of Contents

List of Figures

Chapter 1

Introduction

1.1 Overview

Message dissemination is considered one of the most important applications in VANET. A message is created when an incident has occured and then it is disseminated to the neighbour vehicles. Malicious nodes can alter the messages which may result in fatal losses. In this case, Blockchain can help us to validate these messages and disseminate it efficiently. Blockchain can also store these messages which are almost impossible to modify. Blockchain is a viable option to tackle the message dissemination related challenges faced in implementing VANET in real life. Existing algorithms used in blockchain require modifications to achieve the best performance. We propose a blockchain based system that can help us to utilize the blockchain technology in the best manner in VANET.

In this Chapter, we have briefly discussed the Message dissemination process in VANET, the role of Blockchain in VANET, Challenges faced in this area and the Motivations we had behind our proposed solution, Solution approaches, our Contributions in this area, and finally we conclude the chapter with the Organization of the thesis.

1.2 Message dissemination in VANET

The dissemination of messages in Vehicular Ad-Hoc Networks (VANETs) involves the transmission and propagation of information among vehicles in the network. This process is vital for facilitating efficient communication and coordination among vehicles, supporting applications such as traffic management, collision avoidance, and emergency notifications. However, the distinctive features of VANETs, including high mobility, dynamic network topology and limited communication range, present notable obstacles to achieve effective message dissemination. Overcoming these challenges necessitates the development and implementation of resilient and adaptable communication protocols capable of handling the rapidly changing network conditions. These protocols are crucial for ensuring the dependable and timely delivery of messages to their intended recipients. The validation process involves verifying the integrity

and authenticity of the transmitted messages. It plays a crucial role in ensuring the reliability and trustworthiness of the information exchanged among vehicles. In this process, various techniques and mechanisms are employed to validate the messages and detect any potential tampering or malicious activities. Forwarding plays a vital role in the dissemination of messages within VANETs (Vehicular Ad-Hoc Networks). It involves the transmission of messages from one vehicle to another within the network, ensuring their effective distribution to the intended recipients. The significance of efficient forwarding mechanisms in VANETs stems from the dynamic and rapidly evolving nature of the network topology. In VANETs, forwarding strategies are specifically designed to take advantage of the opportunistic characteristics of vehicle movements. When a vehicle receives a message, it assesses its own position, the content of the message, and the prevailing network conditions. This evaluation helps the vehicle determine the most suitable neighboring vehicle to which it should forward the message. Factors such as proximity, connectivity, and the expected trajectory of nearby vehicles are often considered in this decision-making process. An incentive mechanism can be employed to motivate and encourage vehicles to actively participate in the message dissemination process and create a collaborative and self-sustaining network by providing them with rewards. It discourages dishonest vehicles from participating in the message dissemination process by charging them with a fine. This mechanism aims to incentivize vehicles for relaying and forwarding messages, thus enhancing the overall efficiency and reliability of the network.

1.3 Blockchain in VANET

Blockchain uses blocks to store data, and hash values are used to connect each block to the one before it. Consensus mechanism is a system that the nodes in a blockchain network need to follow, to agree on the validity of the transactions such as Proof-of-Work (PoW), Proof-of-Stakes (PoS) etc. Consensus algorithms are so, one of the most crucial parts of blockchain and it requires a huge amount of attention to be paid. Vehicles need to build trust among each other following some procedures to have successful communication. There are some other critical challenges that need to be addressed, such as broadcast storm, packet collision and computational complexity [5] in blockchain based VANET. So new blockchain based solutions can be developed for VANETs to mitigate the challenges by fully utilizing the blockchain features. Many researches have been conducted to build an effective and efficient trust management system. Overall we can say VANET using blockchain is an open field to research.

The existing consensus mechanisms in their default form are not suitable to use in VANETS. For example, the most common consensus mechanism is Proof-of-Work (PoW) where all nodes

compete with each other to be the miner by calculating a hash puzzle solution which takes about 10 minutes [6]. Due to the high computational cost and long propagation delay of PoW, many alternate solutions were proposed. One alternative consensus mechanism is Proof-of-Stake (PoS), which selects the miner based on the node's stake, considering reputation as a stake [7], [8]. Although it involves less computational complexity, it tends to favor nodes with higher stakes, resulting in bias. In an attempt to introduce fairness, Proof-of-Elapsed-Time (PoET) was introduced, requiring each node to wait for a random period before generating a block. [9] demonstrates its vulnerability in the presence of malicious nodes within the network. The Practical Byzantine Fault Tolerant (PBFT) consensus algorithm is considered highly suitable for VANETs due to its ability to handle high throughput and negotiate message validity [10], [11]. It requires only a threshold number of votes to validate a transaction [12]. Therefore, it operates optimally only when the number of nodes in the network remains below the tolerance level. In VANET, the number of nodes can be higher than this tolerance level of PBFT. So, there is still room for improvement in PBFT to be used in VANET. The selection of relay nodes to disseminate the messages is another critical issue to be addressed. The proper selection of relay nodes ensure the messages will reach all of the other nodes covering the maximum possible distance in the minimum possible time. It will also ensure to minimize the number of broadcast messages by choosing vehicles which are able to deliver message to maximum number of nodes, keeping the quality of the message intact. Incentive mechanisms are needed to incentivize the vehicles which are contributing in the process honestly by verifying the correct blocks and mining the correct blocks. It will encourage honest behaviour in the vehicles and discourage any kind of malicious behaviour.

1.4 Challenges and Motivation

A key challenge in VANET for effective road safety is ensuring minimal latency in message validation and dissemination. Rapid processing is required to avoid learning about incidents after being on the wrong route or having arrived at the location. Voting among neighbor vehicles to achieve consensus can speed up the validation process. However, this approach can cause a broadcast storm, lowering network quality and interfering with system functionality. It is critical to reduce communication overhead by exchanging as few messages as possible within the network. Validation calculations often require a significant amount of computational power which is another aspect that needs to be considered.

Choosing forwarder nodes at each hop level in the message dissemination process requires rigorous calculations that can be time consuming. Reachability and transmission success rate

are important parameters for optimal forwarder selection, but computationally expensive or biased parameters can reduce efficiency. It is critical to select relay nodes capable of covering the greatest distance in the shortest amount of time with the fewest broadcast messages. Reduced overlapping of covered areas improves efficiency even more. Our goal is to develop a consensus algorithm that minimizes validation and dissemination latency while avoiding broadcast storms.

Proof-of-Work (PoW) [23] and Practical Byzantine Fault Tolerant (PBFT) [24] are popular consensus mechanisms for blockchains. PoW is computationally expensive and time-consuming, while PBFT has scalability issues in large networks. In VANET, the network is short-lived due to vehicle mobility, necessitating accurate and fast message validation. However, PoW and PBFT are not directly applicable in VANETs. Implementing these mechanisms can lead to broadcast storms and network congestion. To address these challenges, an efficient consensus mechanism is proposed for blockchain-based VANETs, aiming to reduce the number of messages passed. Balancing message reduction while ensuring accurate calculations is a significant challenge. We take advantage of both PoW and PBFT to introduce an efficient consensus mechanism.

The message dissemination process should select relay nodes strategically to cover the maximum distance in the shortest time using minimal broadcasts. The Proof-of-Quality-Factor (PoQF) introduces Quality Factor for relay node selection. However, biased results and potential overlapping of covered areas remain concerns. Emphasizing message dissemination to the farthest distance rather than a specific hop level is crucial to avoid restricted coverage and poor performance.

Incentive mechanisms are essential to encourage vehicle participation and discourage malicious behavior. We propose an incentive mechanism that considers both monetary units and vehicle reputation, as relying solely on monetary units may not guarantee honest behavior. Incorporating reputation in the validation process enhances its importance to vehicles.

1.5 Solution Approaches

The consensus mechanism aims to validate incident messages in VANET. PoW and PBFT are popular consensus mechanisms for blockchains, but they have limitations in VANETs due to their computational and scalability issues. We propose an efficient mechanism which is a hybrid of both of these mechanisms by leveraging their strengths. Our solution minimizes communication overhead by reducing message exchange and ensures less computational requirements for validation calculations to tackle the limitations of PoW and PBFT.

The PoQF introduces a Quality Factor for relay node selection, but biased results and

overlapping coverage areas are concerns. Efficient forwarder selection relies on parameters like reachability and transmission success rate, but computationally expensive or biased parameters can reduce efficiency. Our message dissemination process selects relay nodes in such a way that the message covers the maximum distance in the shortest time with minimal broadcasts. Our solution also avoids rigorous calculations, which can be time-consuming. PoQF transmits a message up to a specific hop level which restricts coverage and facilitates performance degradation. To solve this, we propose a mechanism that emphasizes message dissemination to the farthest distance.

Incentive mechanism should be designed in a way that it encourages vehicle participation and discourages malicious behavior. Our proposed mechanism considers both monetary units and vehicle reputation to guarantee honest behavior of the vehicles in the system.

1.6 Contributions

In our thesis, we focus on building a blockchain based VANET architecture with a consensus algorithm, a message forwarding mechanism and an incentive mechanism which altogether increases the performance of the system. Our contributions can be summarized as below:

- We proposed an efficient and secure consensus mechanism which utilizes the best practices of PoW and PBFT. It uses selective voting mechanism and weighted sum of votes for the validation purpose which reduces the validation latency. The number of broadcast messages are also reduced, thus it helps to lower the chances of broadcast storm.
- We proposed a message forwarding mechanism which is able to disseminate the validated message to the maximum number of nodes using the minimum number of broadcast messages and the selection process is also simple. The forwarding process is continued until a threshold distance is covered.
- We proposed an incentive mechanism based on both reputation and monetary units. Nodes gets increase in their incentives for their honest behaviour and they get decrease for malicious behaviour. The reputation is also used in the validation process.
- The simulation is done in simulator platform Omnet++ integrated with Sumo. The simulation results are analyzed and they show improvements.

1.7 Organization

The thesis is organized as follows. In Chapter 2, we provide a literature review with a section for background studies on VANET and Blockchain, focusing on their relevance to our thesis. Another section for related works which explores common Consensus Mechanisms and provides an overview of the relevant existing works in this area. In Chapter 3, we present the proposed solution with the problem statement, motivation behind our proposed solution, system model and assumptions and finally the proposed Consensus Mechanism and Message Dissemination Process along with the Incentive Mechanism. In Chapter 4, we analyze the results obtained from the simulation. Finally, in Chapter 5, we conclude the thesis and discuss potential avenues for future research.

Chapter 2

Literature Review

2.1 Background Studies

In this section we give a background study on the relevant topics to our thesis. We discuss about vehicular adhoc network (VANET) including the standards it follows, its architecture, communication types, attacks and the challenges it faces. We also discuss about blockchain including different blockchain types, the architecture of a block, its features and different consensus mechanisms. Finally we discuss about the role of blockchain in VANET.

2.1.1 VANET

By utilizing moving vehicles on roadways as wireless nodes, a Vehicular Adhoc Network (VANET) establishes communication among the cars, thereby forming a dynamic network. The advent of "car-to-car ad-hoc mobile communication and networking" applications in 2001 marked the initial introduction of VANETs. Broadly speaking, VANETs fall within the classification of "wireless adhoc networks," and more precisely, they belong to the realm of "Mobile Adhoc Networks" (MANETs). VANETs provide services in case of preventing collisions, road crossing, route scheduling, safety, traffic monitoring and so on. The main constraints in the network are in the areas of security and scalability. The ever growing importance of VANET also comes with threats of attacks.

As the name implies, the topology of the network in VANET frequently changes as a result of the motion of the cars. Keeping drivers safe on the roadways is one of VANET's primary goals. In this case the cars can have direct connection among themselves or they can communicate indirectly with the help of Road Side Units (RSU), living in a very short range of distance. Whenever any vehicle detects an abnormal activity on the road, it informs other vehicles about it and so the other vehicles can avoid that very unexpected situation. Thus VANET forms a network among cars and helps to relay information among cars.

The "Intelligent Transportation System (ITS)" framework includes VANETs as a vital part. In reality, "Intelligent Transportation Networks" is another term for VANETs. The "Internet of Vehicles," as VANETs later became, was anticipated to become "Internet of Autonomous

Vehicles". By the year 2015, VANETs took a more general term called "Inter-vehicle Communication", which focuses on less involvement of Road Side Units (RSU) or cellular networks.

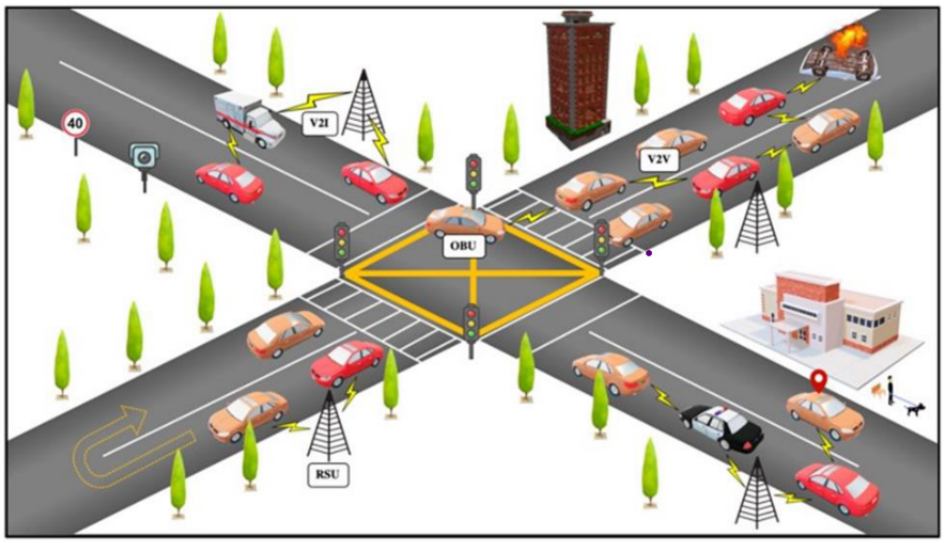

Figure 2.1: Vehicular Ad-hoc Network (VANET) Communication [13]

2.1.1.1 Standards

Standards for VANETs are majorly being formed in the USA, Europe and Japan as they are more advanced in the automotive industry than other countries. There is a Technical Subcommittee in IEEE communications society which works on Vehicular Networks & Telematics Applications (VNTA).

1. DSRC: Many applications based on vehicular communication can be supported by Dedicated Short-Range Communications (DSRC), which is built for this purpose. DSRC deployment is primarily driven by the need to enable accident prevention applications that rely on frequent data transfers between cars (V2V) and between vehicles and roadside infrastructure (V2I). The Federal Communications Commission (FCC) has designated seven channels in the 5.9 GHz spectrum for this use . A shorter span of a few hundred meters is used for communication.

2. WAVE: At the PHY and MAC layers, DSRC utilizes IEEE 802.11p Wireless Access for Vehicular Environments (WAVE), which is an adapted variant of IEEE 802.11 or IEEE 802.11p. Additionally, it incorporates the standards set forth by the IEEE 1609 Working Group. These dedicated channels can be used in multi-channel operation with the WAVE protocol.

2.1.1.2 Architecture

According to the architecture standard guidelines of IEEE 1471-2000 [14,15] and ISO/IEC 42010 [16] the VANET system comprises three distinct domains: the mobile domain, the infrastructure domain, and the generic domain [17].

1. Mobile domain: The mobile domain encompasses both the vehicle domain and the mobile device domain. The mobile device domain includes portable devices like personal navigation devices, smartphones, and similar gadgets. On the other hand, the vehicle domain comprises different types of vehicles such as cars, buses, and more.

2. Infrastructure domain: Within the infrastructure domain, there exist two entities, the central infrastructure domain and the roadside infrastructure domain. The roadside infrastructure domain is composed of elements like traffic lights and other roadside units. Conversely, the central infrastructure domain includes management centers like traffic management centers and vehicle management centers.

3. Generic domain: The generic domain encompasses both the internet infrastructure and private infrastructure. It encompasses a wide range of nodes, servers, and computer resources that directly or indirectly support the VANET system.

2.1.1.3 Communication Types

There are 3 types of communications in VANET, which are Vehicle-to-Vehicle(V2V), Vehicle-to-Infrastructure (V2I) and Inter-Infrastructure communication (I2I).

1. Vehicle-to-Vehicle Communication: In V2V, vehicles communicate with each other exchanging data using the wireless network. Here exchanged data may be speed, location, traffic information etc. It uses Dedicated Short Range Communication (DSRC), thus the communication range is at maximum 300 meters [18].

2. Vehicle-to-Infrastructure Communication: In V2I, communication is done between vehicles and road side infrastructure. It is mainly done to ensure a wider range of mobility. Applications can be used to combine V2V and V2I communication and achieve higher efficiency and also more safety.

3. Infrastructure-to-Infrastructure Communication: In I2I, road side infrastructure units communicate among themselves, resulting in a wider range of communication overall. It offers multi-hop communication and thus increases flexibility in content sharing and increases communication range by a great extent.

2.1.1.4 Attacks

VANET can face many kinds of attacks as it relies on the cooperation of the nodes. The attacks can be classified mainly in 2 types such as:

Passive Attacks

It means the attacker doesn't disturb the network rather collects information for future attacks. Some common types of passive attacks in VANETs are given below:

1. Eavesdropping: Attackers intercept and capture wireless communications between vehicles or between vehicles and infrastructure units. By eavesdropping on these communications, attackers can gain unauthorized access to sensitive information, such as location data, messages, or private user information.

2. Traffic Analysis: Attackers analyze the patterns, frequency, and content of network traffic to gather information about the behavior, routes, or activities of vehicles. This information can be used to infer sensitive details, such as the origin and destination of vehicles or their traveling patterns.

3. Location Tracking: Attackers may monitor and track the movements of specific vehicles by analyzing the location information transmitted in VANETs. This can lead to privacy breaches, stalking, or unauthorized tracking of vehicles.

4. Data Interception: Attackers intercept and capture data packets transmitted over the network. By capturing these packets, attackers can gain access to sensitive information, including personal data, messages, or digital signatures, potentially leading to privacy breaches or unauthorized use of the intercepted data.

5. Identity Theft: Attackers may attempt to steal the identities of legitimate vehicles or infrastructure units by capturing and mimicking their communication patterns or digital signatures. This can enable attackers to impersonate legitimate entities, leading to various security breaches or unauthorized access.

6. Traffic Flow Analysis: Attackers analyze the traffic flow patterns in VANETs to gather information about the density, speed, or distribution of vehicles in specific areas. This information can be used for malicious purposes, such as identifying vulnerable spots or planning targeted attacks.

7. Key Discovery: Attackers may attempt to discover encryption keys or security credentials used in VANETs by analyzing the exchanged messages or capturing cryptographic material. This can lead to unauthorized access, message decryption, or compromise of security mechanisms.

2.1.1.5 Active attacks

In this case the attacker disturbs the network by changing or destroying the data or normal operation of the network. Active attack can be external where the attacker tries to cause congestion in the network or internal where the attacker tries to get access to the network to participate in network activities. Some common types of active attacks in VANETs are given below:

1. Denial of Service (DoS) Attacks: Cyber attackers use DoS attacks with the intention of causing disruptions to network services, making them less available and reliable. This can be achieved by flooding the network with excessive messages, consuming network resources, or exploiting vulnerabilities in communication protocols to cause congestion and communication failures.

2. Sybil Attacks: In Sybil attacks, the attacker resorts to creating multiple fake identities or Sybil nodes in order to seize control or exert influence over the network. By impersonating multiple vehicles, the attacker can manipulate routing protocols, inject false information, and disrupt the network's integrity and operation.

3. Black-Hole Attacks: In a black-hole attack, a sneaky vehicle pretends to offer the shortest or most efficient route to a destination, even though its intentions are malicious. As a result, other vehicles route their traffic through the malicious vehicle, leading to the dropped or misrouted packets and disruption of communication.

4. Wormhole Attacks: In a wormhole attack, malicious nodes establish a virtual tunnel between two distant locations in the network. This enables the attacker to redirect or relay messages through the tunnel, bypassing normal routing protocols. It can lead to incorrect routing decisions, information leakage, and disruption of network services.

5. Jamming Attacks: Jamming attacks involve the intentional interference of wireless signals in VANETs. Malicious attackers send out powerful radio signals on the same frequency band, creating chaos in the communication between vehicles and leading to network congestion or loss of data packets.

6. GPS Spoofing Attacks: In GPS spoofing attacks, attackers manipulate the GPS signals received by vehicles, deceiving them about their actual position or time. By providing false location information, attackers can disrupt navigation systems, mislead vehicles, and cause accidents or confusion on the road.

7. Message Tampering Attacks: Attackers have the capability to intercept and tamper with the content of messages shared between vehicles or between vehicles and infrastructure, potentially altering the information being communicated. By tampering with the messages,

attackers can manipulate the integrity and authenticity of the information, leading to incorrect routing decisions or malicious actions.

8. Replay Attacks: In a replay attack, attackers capture legitimate messages and retransmit them at a later time. By replaying these messages, attackers can deceive vehicles, disrupt communication, or manipulate the integrity of transmitted data.

2.1.1.6 Challenges

As mentioned in [19], VANET faces several kinds of challenges required to be addressed such as:

1. Communication and Connectivity: VANETs require reliable and efficient communication among vehicles and between vehicles and infrastructure. However, the high mobility of vehicles, varying traffic conditions, and frequent network topology changes pose challenges in establishing and maintaining stable connectivity.

2. Network Scalability: VANETs need to handle a large number of vehicles, which can result in scalability issues. Efficient routing and addressing mechanisms are essential to manage the increasing number of vehicles and ensure effective communication.

3. Mobility management: Due to moving cars the network topology on VANET changes very fast. Again in an adhoc infrastructure there is no fixed infrastructure to rely on. That's why traditional mobility management protocols fail to serve sufficiently here.

4. Security and Privacy: VANETs are vulnerable to security threats, including malicious attacks, unauthorized access, and data tampering. Ensuring the security and privacy of communication, as well as protecting the integrity of data transmitted in the network, is a significant challenge.

5. Reliable routing: As we have seen, network traffic in VANET is greatly unpredictable which is again location dependent. For these reasons traditional routing protocols fail to serve here.

6. Data Management: VANETs generate a vast amount of data, including traffic information, location updates, and multimedia content. Efficient data management, storage, and dissemination techniques are necessary to handle this data overload and ensure timely and relevant information delivery.

7. Authentication: In the case of a security framework a secure and lightweight authentication algorithm is needed to check the authenticity of VANET nodes and messages. False messages may even cause death to passengers.

8. Quality of Service(QoS): QoS is hard to integrate in VANET as the parameters in

this case such as packet delivery ratio, end to end delay etc are dependent on factors such as handoff latency, congestion, collision etc.

2.1.2 Blockchain

Blockchain is essentially a digital record-keeping system that operates in a decentralized manner. It acts as a shared public ledger where various digital events are recorded and stored among participating nodes. To add new records to the ledger, they must first be validated and approved by a majority of the nodes in the network, ensuring consensus. Each block in the blockchain contains a unique identifier, known as a hash value, which is derived from the previous block in the chain. This process of linking blocks together creates a secure and tamper-resistant chain of information. The key concept behind blockchain technology is decentralization, meaning that every participant in the network possesses a copy of the ledger. Whenever a new block is added to the chain, it is propagated across the peer-to-peer network, ensuring that all nodes stay updated. Unlike traditional methods of data storage and transfer, blockchain is not duplicated or transferred; instead, it is distributed among the network participants. One of the notable features of blockchain is its transparency. Any changes or updates made to the blockchain are visible to all participants in the network. This transparency helps preserve trust and integrity as everyone can verify the history and authenticity of transactions or events recorded on the blockchain.

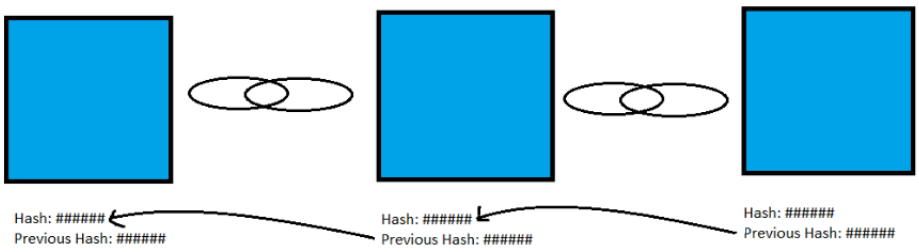

Figure 2.2: An example of Blockchain

2.1.2.1 Blockchain Types

Blockchain can be mainly of four types, along with other additional types such as:

1. Public: The public blockchain encourages anyone to join and actively contribute to its operations.Thus, it is called permission-less and non restrictive. As it is public, alteration is

impossible. So, it is trustable, secure, open and transparent. It is used in voting and fundraising.

2. Private: In private blockchain the permission is given only to selected nodes. Thus it is called permissioned and restrictive. It is also smaller than public blockchain. That's why it's faster and can be scaled easily. It is used in internal voting, asset ownership and supply-chain management.

3. Hybrid: The hybrid blockchain is a hybrid of the previous two types. It's for those who want the best of the previous two. Thus its secure and cost effective. It is used in real estate, retail etc.

4. Consortium: Similar to hybrid blockchain but it is controlled by a group of people. Only the predetermined nodes control the consensus mechanism. It is secure but it lacks transparency. It is used in banking and payments, research and food tracking.

5. Permissioned Blockchain: Permissioned blockchains require participants to obtain permission or credentials to join the network and validate transactions. They offer more control and privacy compared to public blockchains but are still decentralized to some extent. Permissioned blockchains are commonly used in enterprise settings, where trust and compliance requirements are essential.

6. Permissionless Blockchain: Permissionless blockchains, also known as public blockchains, do not require participants to obtain permission or credentials to join the network. They offer high decentralization, transparency, and censorship resistance. Permissionless blockchains are open to anyone and allow for a greater level of innovation and participation.

7. Sidechain: Sidechains are separate blockchains that are interoperable with the main blockchain. They allow for the execution of specific applications or use cases while leveraging the security and consensus of the main blockchain. Sidechains provide scalability and flexibility for blockchain networks.

8. Blockchain-as-a-Service (BaaS): BaaS refers to cloud-based services that enable organizations to develop, deploy, and manage blockchain applications without the need to set up and maintain their blockchain infrastructure. BaaS platforms simplify the development process and provide ready-to-use blockchain frameworks.

2.1.2.2 Block

At its core, blockchain is like a chain made up of interconnected blocks. The very first block in a blockchain, known as the genesis block, holds information that is universally accessible and recognized by all nodes involved in the network. It serves as the foundation upon which subsequent blocks are added, forming the chain of interconnected information. The block is

made of 2 main parts,

2.1.2.3 Block Header

Within a block, there exists a block header that stores crucial metadata about the block itself. This metadata includes details such as the block's version number, timestamp indicating when it was created, the hash value of the previous block in the chain, and a nonce (essentially a randomly generated number utilized in the mining process). These pieces of information collectively contribute to the structure and integrity of the blockchain. The header part consists of 6 parts:

1. Version number: The version number of a block in a blockchain refers to the identifier or indicator that denotes the specific version or format of the block's data structure. It indicates the rules and protocols used for creating and interpreting the block. By having a version number, blockchain networks can introduce changes or improvements to the block structure while maintaining backward compatibility with previous versions. It allows for upgrades or modifications to the blockchain's functionalities without disrupting the existing blocks and their interpretation. The version number may be represented as an integer or a combination of numbers and letters, depending on the specific blockchain protocol.

2. Hash of the previous block: A hash can be described as a special digital fingerprint created by using a cryptographic hash function on the block header. It acts as a unique digital signature for the block, playing a crucial role in both preserving the block's integrity and connecting it to the previous block in the chain. When it comes to reaching consensus in the blockchain network, the hash is employed to validate and authenticate the block's genuineness. The SHA-256 cryptographic hashing algorithm is used to generate this secure and reliable hash value.

3. Root hash of the Merkel tree: The root hash of the Merkle tree plays a significant role in the blockchain, serving as the ultimate representation of all the transactions contained within a block. To derive this root hash, a series of hash operations are performed on the individual transactions and their intermediate hash values. The Merkle tree can be visualized as a hierarchical structure, resembling a binary tree. Starting from the lowest level, each transaction is individually hashed. These transaction hashes are then combined and hashed together in pairs, creating a new level of hash values known as intermediate hashes. This process continues, moving up the tree, until eventually a single hash remains at the top—the Merkle root or root hash. By comparing a transaction's authenticity with the root hash, one can efficiently verify its validity. This efficient verification process adds an extra layer of security

to the blockchain and ensures the integrity of the transactions within.

4. Block Height: In blockchain, block height refers to a numerical value assigned to each block, signifying its position within the chronological sequence of the blockchain. It acts as a sort of level indicator, depicting the number of blocks that precede the given block. The block height begins at 0 for the genesis block, which marks the initial block in the blockchain, and subsequently increases by one for each new block added. This systematic numbering ensures that blocks are meticulously arranged in a sequential order, creating an unbroken chain. The determination of a block's height relies on the consensus algorithm implemented in the blockchain network. This algorithm governs the processes of block creation and validation. By following the consensus rules, the blockchain network maintains consistency and synchronization, guaranteeing that blocks are added to the chain in an organized and reliable manner.

4. Time in seconds: The timestamp within a block of a blockchain holds the precise moment when the block came into existence and joined the blockchain. It acts as a timestamp that records the block's creation time and aids in establishing the accurate chronological sequence of blocks within the blockchain. This timestamp carries significant importance in upholding the integrity and security of the blockchain system. By incorporating timestamps, the blockchain ensures that blocks are added in a precise, time-stamped, and sequential manner. This meticulous approach thwarts any attempts to manipulate or tamper with the order of blocks. The timestamp serves as a safeguard, preserving the authenticity and reliability of the blockchain's chronological flow.

5. The goal of the current difficulty: The objective of the current difficulty level within a block of a blockchain is to carefully regulate the pace at which new blocks are added to the blockchain. The difficulty adjustment mechanism seeks to maintain a consistent and predetermined interval for block creation. This is accomplished by setting the difficulty level, which determines the computational effort miners must exert to discover a valid block hash. Periodic adjustments are made to the difficulty level in order to control the rate at which new blocks are added. The specific aim of this adjustment is to achieve a target block creation time. If blocks are being mined too rapidly, the difficulty level increases, presenting miners with more challenging puzzles. On the other hand, if blocks are being mined too slowly, the difficulty level decreases to simplify the puzzles. The difficulty adjustment algorithm strives to strike a balance between the overall computational power of the network and the desired rate of block creation. By carefully calibrating the difficulty level, the blockchain network ensures a sustainable and controlled growth of the blockchain while optimizing the utilization of computational resources.

6. Nonce: The nonce (number used once) plays a vital role in the mining process of a

blockchain. It is a randomly generated value that gets added to the block header. Miners engage in a repetitive process of modifying the nonce until they discover a hash that satisfies specific criteria, such as having a specific number of leading zeros. The purpose of the nonce is to introduce an element of randomness into the mining process, making it computationally demanding to find a valid block hash. By adjusting the nonce value, miners effectively alter the input data provided to the hash function. Their goal is to search for a hash that falls within the target range set by the network's difficulty level. Through this iterative process, miners utilize the nonce to pursue a valid hash that fulfills the requirements and solves the cryptographic puzzle at hand. It is this successful solution that enables them to add the block to the blockchain, ultimately contributing to the secure and trustworthy functioning of the entire blockchain system.

2.1.2.4 Block Body

Within a blockchain, the block body encompasses the essential segment of a block, housing the real data or information that is stored or shared across the blockchain network. It comprises diverse components that are tailored to the specific implementation of the blockchain and the nature of the data being handled. The block body usually includes:

1. Transactions: In most blockchain networks, the primary purpose is to record and validate transactions. Therefore, the block body contains a list of transactions, each representing a transfer of value or an action performed on the blockchain. Each transaction includes details such as the sender, recipient, amount, and any additional data associated with the transaction.

2. Smart Contract Code: In blockchain platforms that support smart contracts, the block body may include the code or bytecode of the smart contracts being executed. This code defines the rules and conditions that govern the behavior of the smart contract when invoked.

3. State Changes: When transactions or smart contracts are executed, they may result in changes to the state of the blockchain. The block body can include information about these state changes, such as updates to account balances, contract storage, or other relevant data structures.

4. Metadata: The block body may contain additional metadata related to the block itself, such as the block header, timestamps, nonce, and references to previous blocks, enabling the block to be linked to the blockchain's history.

The block body, alongside components such as the block header, fulfills a critical function in upholding the integrity and ensuring the continuity of the blockchain. These essential elements work hand in hand to safeguard the reliability and coherence of the entire blockchain system.

Miners or validators verify the transactions and data within the block body to ensure their validity and consensus rules. By including the relevant data within the block body, the blockchain network creates a transparent and immutable record of transactions or actions, enabling secure and decentralized storage, verification, and retrieval of information. It's important to note that the specific structure and content of the block body can vary depending on the blockchain platform and its design choices. Different blockchain networks may have different data structures, protocols, and features, resulting in variations in the composition and organization of the block body.

2.1.2.5 Addition of New Block

There are some general steps involved in adding a new block to the blockchain, which are given below:

1. Transaction Collection: Transactions are collected from various participants or nodes in the network. These transactions represent actions or data that need to be recorded on the blockchain. The transactions can include transfers of assets, smart contract executions, or other relevant data.

2. Transaction Verification: The collected transactions undergo a verification process to ensure their validity. This verification typically involves checking the transaction's digital signatures, confirming that the sender has sufficient funds or permissions, and validating any other specified conditions or rules.

3. Block Construction: After the transactions undergo verification, they are grouped together to construct a fresh block. This block comprises two primary components: the block header and the block body. The block header holds crucial metadata such as the block number, timestamp, and reference to the preceding block. On the other hand, the block body encompasses the verified transactions themselves, along with any pertinent data associated with them.

4. Block Mining: Within proof-of-work (PoW) blockchain networks, miners engage in a competition to solve a computational puzzle. They do so by continually adjusting the nonce value of the block and calculating its hash. The objective is to discover a hash that satisfies the network's predetermined difficulty target. As soon as a miner successfully finds a valid hash that fulfills the requirements, they are able to create a new block and add it to the blockchain.

5. Consensus and Validation: Once a new block is successfully mined, it is promptly shared with the entire network. Other nodes within the network undertake the crucial task of validating the block's legitimacy. They do so by independently verifying the included transac-

tions, confirming the proof of work, and ensuring that the block aligns with the consensus rules of the blockchain. Consensus mechanisms, such as proof-of-work (PoW), proof-of-stake (PoS), or other established algorithms, play a pivotal role in facilitating agreement among the nodes regarding the validity of the freshly mined block.

6. Block Addition: Upon receiving validation from the network's consensus, a valid block is accepted and appended to the blockchain. Through its reference to the previous block, a solid connection is established, forming an unalterable chain of interconnected blocks. Once added to the blockchain, the transactions enclosed within the block are considered officially confirmed and permanently embedded in the historical records of the blockchain.

7. Block Propagation and Synchronization: The recently incorporated block is disseminated to other nodes within the network, enabling them to uphold synchronization. All participating nodes undertake the task of updating their local copies of the blockchain to encompass the newly added block. This process guarantees that all nodes possess an accurate, current, and harmonized perspective of the blockchain, ensuring consistency across the network.

2.1.2.6 Blockchain Features

The main features of blockchain are immutability, privacy, transparency and decentralization as described below:

1. Immutability: Immutability stands as a foundational attribute of a blockchain, ensuring that once data is incorporated, it becomes exceptionally challenging to modify or erase. Within each block, a cryptographic hash is formed by combining the data contained in the block with the hash of the preceding block. Consequently, any attempt to modify the data within a block necessitates recalculating the hash for that specific block as well as all subsequent blocks, making tampering with the data extremely difficult. This immutability provides reliable data storage and enhances the integrity of the blockchain.

2. Privacy: Blockchain relies on the power of cryptography to safeguard transactional privacy. Every individual engaged in the blockchain network possesses a distinctive set of cryptographic keys comprising a public key and a private key. The public key is openly accessible to all participants, enabling them to validate transactions and engage with the network. Conversely, the private key remains confidential and exclusively known to its rightful owner. This private key assumes the critical role of digitally signing transactions, imparting authentication and ensuring that solely authorized entities can access or alter the linked data. Through this cryptographic mechanism, blockchain maintains the privacy and security of transactions. This cryptographic mechanism helps protect the privacy of sensitive information in blockchain

transactions.

3. Transparency: Blockchain fosters transparency by storing all transactions within a shared and decentralized ledger. Each participant in the blockchain network possesses a complete copy of the transaction history, facilitating open access for anyone to observe and authenticate the transactions. This transparency inherent in the blockchain technology establishes a robust framework for accountability and trust among participants. It empowers auditing of transactions, enabling all parties to monitor and validate the integrity of the data. The transparent nature of blockchain cultivates a heightened level of confidence in the system, promoting a secure and accountable environment for all involved.

4. Decentralization: Decentralization stands as a pivotal principle within blockchain technology. Rather than depending on a central authority, blockchain functions as a network of interconnected nodes, with each node preserving a complete copy of the entire blockchain. To validate and establish consensus on the state of the blockchain, consensus algorithms like Proof-of-Work (PoW) or Proof-of-Stake (PoS) come into play, ensuring agreement among all participating nodes. By embracing decentralization, blockchain disperses authority and empowers a collective network to govern the integrity and operations of the technology. This decentralized approach eliminates the need for a single point of control, making the blockchain resistant to single points of failure, censorship, and manipulation. Decentralization enhances the security, resilience, and trustworthiness of the blockchain network.

5. Security: Blockchain networks employ cryptographic algorithms to secure the data and transactions. These algorithms serve to safeguard the data stored within the blockchain, shielding it from unauthorized access, tampering, or fraudulent activities. The decentralized nature of blockchain imparts an additional layer of security, as the network hinges on consensus mechanisms to authenticate transactions. By engaging in a collective validation process, the blockchain fosters a resilient and secure environment, fortifying the integrity and reliability of the stored data.

6. Distributed Ledger: Blockchain functions as a distributed ledger, with numerous nodes within the network maintaining multiple copies of the blockchain. This redundancy ensures that even if some nodes fail or malicious actors attempt to alter data, the integrity of the blockchain is preserved.

7. Smart Contracts: Smart contracts embody self-executing agreements that encapsulate the terms and conditions within their code. By automating and enforcing predefined rules and agreements, they eliminate the requirement for intermediaries. Blockchain platforms that accommodate smart contracts provide the foundation for developing decentralized applications

(DApps) and facilitate intricate transactions and interactions.

8. Privacy and Pseudonymity: While blockchain is often associated with transparency, certain blockchain implementations incorporate privacy features. These features allow participants to maintain their privacy while still engaging in secure and auditable transactions. Methods like zero-knowledge proofs and encryption can be employed to augment privacy and pseudonymity within the blockchain.

9. Scalability: Blockchain technology has faced challenges with scalability, especially in public blockchains. However, various scaling solutions and advancements, such as sharding, layer 2 protocols, and consensus algorithm improvements, are being developed to enhance the scalability of blockchain networks, allowing them to handle a larger number of transactions and accommodate growing user bases.

10. Interoperability: Interoperability encompasses the capacity of diverse blockchain networks to communicate and cooperate effortlessly with one another. Interoperability solutions strive to streamline the exchange of assets, data, or services across multiple blockchains, fostering improved collaboration and connectivity between distinct blockchains. By enabling seamless interaction, these solutions empower different blockchain networks to work harmoniously together, expanding the possibilities for shared functionalities and collective advancements.

11. Consensus Mechanisms: In blockchain networks, consensus mechanisms play a vital role in verifying transactions and establishing agreement on the state of the blockchain. Various consensus mechanisms, such as Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT), provide different levels of security, efficiency, and decentralization. These mechanisms ensure that transactions are authenticated and that the blockchain operates smoothly and reliably, while allowing for flexibility in choosing the most suitable consensus approach for a given blockchain network.

These features collectively contribute to the unique capabilities and benefits of blockchain technology, enabling trustless and secure peer-to-peer transactions, decentralized applications, and novel business models across various industries.

2.1.2.7 Consensus Mechanisms

A consensus mechanism refers to a system that governs how nodes in a blockchain network reach agreement on the legitimacy of transactions. This mechanism guarantees that only valid transactions are incorporated into the blockchain and that all copies of the blockchain possess the complete set of valid transactions. By adhering to the consensus mechanism, the blockchain network ensures a unified and consistent view of the transactions, establishing trust and in-

tegrity in the system. The computer nodes that work on the validation of the transactions are called miners. Consensus mechanism ensures that all these miners agree on the validity of the new transactions. For example, if I buy one bitcoin and transfer it to my cryptocurrency wallet then everyone must agree that it is my bitcoin. Otherwise, the bitcoin will be worthless. There are many different types of consensus mechanisms being used in blockchain technology nowadays. Some of them are depicted here:

1. Proof-of-Work (PoW): In a Proof of Work (PoW) consensus mechanism, miners engage in a competitive process to authenticate new transactions within the blockchain network. The one that validates at first among them, gets to form a new block, confirming transactions and also it earns a reward. This is the most commonly used consensus mechanism but it is highly energy intensive. Popular cryptocurrencies like Bitcoin and Ethereum rely on this consensus mechanism for their operation.

2. Proof-of-Stake (PoS): In PoS, the node with the largest holding of the network's currency validates the new transactions and earns reward. PoS is energy-efficient compared to PoW and provides more scalability. Ethereum is transitioning from PoW to PoS with its Ethereum 2.0 upgrade. It makes it possible to have faster and lower cost transactions but it is some sort of biased.

3. Delegated Proof of Stake (DPoS): Delegated Proof of Stake (DPoS) is a consensus mechanism that merges the benefits of Proof of Stake (PoS) with a representative model. In DPoS, token holders participate in voting to select a small group of delegates, also known as block producers. These delegates assume the responsibility of creating blocks and validating transactions. DPoS facilitates quicker block confirmation times and supports high transaction throughput, making it an efficient consensus mechanism. Examples of DPoS-based blockchains include EOS and TRON.

4. Practical Byzantine Fault Tolerance (PBFT): Practical Byzantine Fault Tolerance (PBFT) is a consensus mechanism specifically developed for permissioned blockchains. It necessitates a pre-established group of nodes, known as replicas, to collectively agree upon the sequencing of transactions. PBFT ensures a reliable consensus among the authorized nodes, contributing to the overall security and integrity of the permissioned blockchain network. PBFT can tolerate a certain number of malicious nodes (Byzantine faults) while ensuring agreement among honest nodes. Hyperledger Fabric, for instance, uses a variation of PBFT as its consensus algorithm.

5. Proof-of-Elapsed Time (PoET): Proof of Elapsed Time (PoET) operates by generating a random wait time for each node in the network. The node that possesses the shortest

wait time gains the opportunity to add the block to the blockchain. PoET ensures an equal and fair chance for every participating node to be selected. This consensus mechanism consumes less power compared to Proof of Work (PoW) and offers improved energy efficiency, making it a more sustainable choice for blockchain networks.

6. Proof of Authority (PoA): In Proof of Authority, consensus is based on a group of pre-approved validators who are known and trusted. These validators take turns producing blocks, and their identity is tied to their reputation. PoA provides fast block confirmation times and is suitable for private or consortium blockchains where trust among participants is established. Examples include VeChain and POA Network.

7. Federated Byzantine Agreement (FBA): FBA is a consensus mechanism in which a consortium of trusted validators collaboratively achieves consensus regarding the sequential arrangement of transactions. Each validator can choose a subset of other validators they trust. Stellar, a blockchain platform, utilizes the FBA consensus algorithm to achieve consensus among its network participants.

2.1.3 Blockchain in VANET

In many of the studies [20–22] we can see blockchain technology can indeed offer a solution to address the challenges faced in Vehicular Adhoc Networks (VANETs) by providing decentralization, transparency, protection, anonymity, and privacy.

One of the challenges in VANETs is the need for authentication algorithms to verify the identities of nodes and messages. Blockchain, with its consensus algorithm, can provide a robust mechanism for authentication and validation. By leveraging a distributed network of nodes, blockchain ensures that transactions and messages are verified by consensus, enhancing the security and trustworthiness of VANETs. Decentralization is crucial in VANETs to prevent unfairness and central points of failure. Blockchain's decentralized architecture, where every node holds a copy of the entire blockchain, eliminates the need for a central authority. This decentralized approach ensures that no single entity has control over the network, enhancing the resilience and reliability of VANETs.

Unauthorized access and attacks are significant concerns in VANETs. Blockchain's tamper-proof nature and cryptographic techniques can help prevent unauthorized access and maintain the integrity of the network. By using cryptographic keys and digital signatures, blockchain ensures that only authorized entities can access and modify the data in the network, mitigating the risk of attacks and ensuring data security. In VANETs, anonymity and privacy are vital to protect the identities and sensitive information of vehicles. Blockchain technology can provide

anonymity by encrypting and hiding the identities of vehicles from malicious nodes. Through the use of cryptographic techniques, blockchain ensures that transactions and interactions are pseudonymous, protecting the privacy of participants in the VANET ecosystem.

Furthermore, blockchain's shared and distributed ledger allows any node in the network to view the transaction history and data, ensuring transparency. This transparency enables auditing, accountability, and trust among participants in the VANET, as the integrity of transactions can be verified by any node at any time.

These contributions of blockchain in VANETs highlight its potential as a powerful solution to address the challenges faced in the domain. By incorporating blockchain technology, VANETs can benefit from enhanced security, decentralized control, transparent transactions, protection against unauthorized access, anonymity, and privacy. Overall, blockchain offers a promising solution to overcome the obstacles and improve the efficiency and reliability of VANETs.

2.2 Related Work

In this section we discuss about some of the most relevant works done in our interested area which includes commonly used consensus mechanisms Proof-of-Work (PoW), Practical Byzantine Fault Tolerance (PBFT) and some other works done by different authors.

2.2.1 Proof-of-Work (PoW)

The most commonly used consensus algorithm in blockchain systems is Proof-of-work(PoW). It was first introduced by Satoshi Nakamoto as a key component of Bitcoin [23]. The primary objective of PoW is to detect malicious activities and ensure security, integrity of the blockchain network.

The process of PoW starts by the participants or miners competing against each other to solve a complex mathematical puzzle. The puzzle requires significant computational power and resources to solve, but the solution can be easily verified by other participants. The process of solving the puzzle is known as mining. The participants who can successfully solve the puzzle receives rewards or incentives for their work. To solve the puzzle the participants have to find a hash value that satisfies certain predefined criteria. Miners use their computational power to repeatedly hash a block of transactions together with a random number called a nonce until they find a hash that meets the criteria. This requires miners to make numerous attempts by varying the nonce value until they find a suitable hash. The difficulty of the puzzle is adjustable and it is designed to maintain a constant rate of block generation in the blockchain network. As more miners join the network, the computational power increases, and the puzzle becomes more difficult. Similarly, if miners leave the network, the computational power decreases and the puzzle difficulty decreases, which ensures that new blocks are added to the blockchain at the predefined rate. Once a miner finds a solution to the puzzle, they broadcast the new block to the network. Other participants can now verify the solution by checking the hash and confirming that it meets the required criteria. If the solution is valid, the block is added to the blockchain, and the miner is rewarded with cryptocurrency tokens.

An important benefit of Proof-of-Work (PoW) is its capability to safeguard against Sybil attacks, which occur when an attacker generates multiple identities in an attempt to seize control of the network. Since solving the puzzle requires substantial computational resources, an attacker would need to control a significant portion of the total computational power in the network, known as the majority or 51% attack, to manipulate the blockchain's history. This makes PoW networks highly secure against such attacks.

Along with the advantages, PoW have certain drawbacks too. The most notable is its high

energy consumption due to the computational power required for solving the puzzle. This has led to concerns about the environmental impact of PoW-based cryptocurrencies. PoW networks are also vulnerable to centralization due to their dependence on computing power. It is because large-scale mining operations with abundant resources have a greater probability of mining new blocks and might therefore result in a concentration of power.

Despite these limitations, PoW remains the most widely used consensus algorithm, particularly in the context of blockchain networks. Its robust security properties and resistance to attacks have made it a popular choice for many cryptocurrencies and blockchain applications.

2.2.2 Practical Byzantine Fault Tolerance (PBFT)

Practical Byzantine Fault Tolerance (PBFT) is a consensus algorithm designed to achieve consensus in distributed systems where a certain number of nodes may be faulty or malicious. It was first introduced by Miguel Castro and Barbara Liskov in 1999 as a solution to the Byzantine Generals Problem [24].

The objective of Practical Byzantine Fault Tolerance (PBFT) is to enable a decentralized network of nodes to collectively agree on the order and authenticity of transactions, even in the presence of nodes that may be faulty or malicious. PBFT operates under the assumption of a partially synchronous network, where there is a predetermined limit on message transmission delays. The consensus process in PBFT is structured into multiple rounds, each comprising several phases. To ensure consensus, a minimum of 3f + 1 nodes are required, where f represents the highest number of faulty nodes that the algorithm can handle while preserving consensus.

The PBFT consensus process unfolds in the following manner: The client initiates the process by sending a request message to the primary node, which serves as the leader for a specific round. Subsequently, the primary node disseminates a pre-prepare message to the other nodes in the network, conveying the proposed request and round information. Upon receiving the pre-prepare message, the remaining nodes validate its authenticity and integrity. If deemed valid, they respond by sending a prepare message, indicating their preparedness to commit the proposed request. Once a node collects 2f prepare messages (where f represents the maximum number of faulty nodes), it broadcasts a commit message, denoting its intention to commit the request. When a node receives 2f + 1 commit messages, it considers the request as officially committed and proceeds to execute it. The outcome of the execution is then relayed back to the client. Lastly, the client provides acknowledgment of the request's execution, thereby finalizing the consensus process for that particular round.

PBFT provides several desirable properties, including safety, which guarantees that all cor-

rect nodes agree on the same order of requests, and liveness, which ensures that requests are eventually executed as long as a sufficient number of nodes are correct and the network is partially synchronous. One of the advantages of PBFT is its relatively low communication complexity. Compared to PoW or PoS algorithms, PBFT requires fewer computational resources and has a faster finality time. It is well-suited for use cases that prioritize low-latency transactions and high-throughput requirements.

PBFT has some limitations when the number of nodes in the network is high. As the number of nodes increases, PBFT's performance can degrade due to the increased message complexity and the need for nodes to communicate and reach agreement. The algorithm requires a quadratic number of messages to be exchanged among nodes in each round, which can lead to scalability issues in large networks. PBFT's performance may suffer when the number of nodes surpasses a certain threshold, impacting its efficiency and practicality for highly decentralized systems. Therefore, PBFT is often more suitable for smaller networks or environments where the number of participating nodes can be managed and controlled. Again, it assumes that the majority of nodes are honest, and its performance degrades significantly when more than f faulty nodes exist. PBFT is also more vulnerable to network delays and can suffer from higher message overhead compared to other consensus algorithms.

Despite these limitations, PBFT has been widely used in various permissioned blockchain frameworks and systems where a known and trusted set of nodes can be established. It provides a practical solution for achieving consensus in distributed systems with Byzantine faults, ensuring the integrity and reliability of the blockchain.

2.2.3 Proof-of-Quality-Factor (PoQF) based Blockchain and Edge Computing for Vehicular Message Dissemination

Most of the consensus algorithms require the assistance of edge computing servers for implementation of VANETs. Consensus algorithms like Proof-of-Work need a long time to run that cannot efficiently support the short-period connectivity issue in VANET [25]. Proof-of-Stake is based on the number of stakes held by each node and thus it is biased [26,27], whereas Proof-of-Elapsed-Time cannot ensure high security against attackers [28]. In PBFT the threshold value of messages required to validate a message is not network adaptable. As a better solution, another consensus algorithm was proposed called Proof-of-Quality-Factor (PoQF) [29]. It is based on voting and these votes are monitored by the edge computing servers. This consensus algorithm takes the help of probability to assess channel quality between the sender and receiver during the selection process.

In the PoQF consensus mechanism, the process comprises four stages. In the first stage, the incident's initiator sends a message, while the nodes receiving and responding to this message are referred to as mining nodes. These mining nodes proceed to create a microblock at the second level, which encompasses the vote for message validation and the Quality Factor (QF) necessary to become a potential relay node. Subsequently, the nodes wait for a randomized period before announcing their microblock. This random waiting time serves several purposes: preventing simultaneous transmission by all nodes, allocating shorter waiting times to nodes with higher QF values, and ensuring randomization when vehicles possess the same QF. By doing so, the random waiting time mitigates packet collisions arising from various causes. Moving on to the third stage, a relay node is selected if it has received a minimum threshold number of microblocks featuring an identical vote as its own and possesses the highest quality factor among all specific microblocks. If the message is authenticated as true, the relay node proceeds to transmit the message, leading to the generation of a keyblock that verifies the message's validity. Conversely, if no node obtains the threshold number of microblocks with a matching vote, the message is labeled as false, and the mining node with the highest quality factor among those who voted false generates a corresponding keyblock. In the final stage, the message continues to be disseminated as long as it remains valid according to the mining nodes and the hop count remains below the maximum threshold. The Quality Factor (QF) calculation is determined by two factors: the Quality of Signal-to-Interference-plus-Noise Ratio (Q(SINR)) and the Distance Factor (DF). Q(SINR) represents the likelihood of successful transmission from a node to all its neighboring nodes, while DF represents the probability that the distance between a node and the sender exceeds a specific threshold required for successful transmission over longer distances.

The PoQF consensus mechanism incorporates an effective approach that involves a mechanism for distributing incentives to reward honest nodes and penalize dishonest ones. In this mechanism, the originator of an incident pays a compensation credit as a form of reimbursement. If the message is successfully validated, a portion of this credit is distributed among the honest mining nodes at the first hop level. Another portion of the credit is allocated to relay nodes if the message is validated as true. However, if the message is found to be false, this portion of the credit serves as a penalty charge and is directed towards regulation authorities. Furthermore, an additional credit is charged to mining nodes that vote against a true incident message. This measure aims to discourage voting against genuine incidents and promote the rapid dissemination of truthful messages. The accumulated additional credit is subsequently awarded to the node responsible for generating the last keyblock pertaining to a specific inci-

dent. The amounts of charges are regularly updated by edge computing servers based on the requirements of each situation, ensuring flexibility and adaptability in the incentive distribution process.

The simulation is performed in Omnet++, using c++ language. In this proposed method, failure in validation is reduced by 15% and 11% compared to PoET and PoS, whereas speed increased by 68ms compared to PoET. It is also seen in the simulation that the number of forks in PoQF is less than PoET and PoS. But PoQF is vulnerable to malicious nodes, the same as PoW, if 50% members of the mining group are malicious. However, PoQF is not dependent on the presence of 2f + 1 mining nodes as in PBFT.

2.2.4 A Light-weight Blockchain Architecture for VANET with verification method and a consensus mechanism (PoVS-BFT)

Many peer-to-peer decentralized data sharing models have been proposed, but most of them could not deal with unauthorized data access issues and also could not provide highly effective verification and validation methods. The authors of this paper came up with a proposal for a new lightweight vehicular blockchain architecture that provides an effective verification model along with a computationally cheaper consensus mechanism called PoVS-BFT [30]. This is a decentralized data sharing model for vehicular edge networks using blockchain where knowledge can be shared without exchanging sensitive information. A two-step verification process is proposed for detecting forged messages and repudiatory activities.

In this context, trustworthiness refers to the vehicle's adherence to its assigned role, and this trustworthiness is overseen by the Roadside Units (RSUs). To assess the trustworthiness of a vehicle, each RSU constructs a naïve Bayesian network specific to that vehicle. These networks consist of a single root node, which can be assigned a value of either 1 (representing trustworthiness) or 0 (representing untrustworthiness). The leaf node represents the vehicle's utility in different roles. The proposed solution handles two insider attacks: Byzantine Attacks and Inference Attacks using its threat model. Each transaction goes through two steps to be verified, they are the endorsement and verification step within a specific period. For Endorsement, peer vehicles are endorsers and for verification, RSUs work as verifiers. The algorithm for the transaction verification process takes a transaction (Tx) as input and the output is whether it is valid or invalid. Vehicle proposes Tx and while time, t is less than the predefined time limit, the endorsers will endorse the Tx. If the RSU verifies the identity and trustworthiness of the transaction and endorsing entities, and if the trust value of each entity involved exceeds a predefined threshold, the transaction (Tx) is considered valid. Otherwise, it is deemed invalid.

This architecture consists of five distinct entity types, where each entity can fulfill one or multiple roles simultaneously. These entities include the client, endorsing peer, non-endorsing peer, verifier, and miner. Here, vehicles can be client, endorsing, and non-endorsing peers. RSUs can be verifiers and miners. Clients do not receive blocks, whereas endorsing and non-endorsing peers can receive them.

In the initial stage of the proposed protocol, the ratings of each RSU/mining candidate are calculated, taking into account the quality and efficiency of the provided service. The satisfaction or dissatisfaction of a service is determined by the requesting vehicle. Each vehicle (v_i) shares its ratings with the certificate authority (CA), which then aggregates, calculates, and broadcasts a ratings set across the network. This set contains tuples of service ratings of RSUs and the number of vehicles that requested services from each RSU during a specific period. In the following phase, a mining committee is formed based on this ratings set. The elimination phase employs a clustering algorithm to divide the mining candidates into two groups. The eligible group is determined by selecting clusters with the highest average service ratings. The validation phase utilizes euclidean distance and service rating-based outlier detection. RSUs with service ratings higher than the average service rating and with Euclidean distances within a tolerance level are included in the consensus committee. The consensus committee then employs a traditional BFT-based consensus procedure to commit blocks in the network.

PoVS-BFT addresses the issue of scalability in vehicular networks by reducing the size of the consensus committee, which results in a decrease in system complexity. The reduction in size, from $O(m^2)$ to $O(p^2)$, significantly improves efficiency. Here, m and p represent the sizes of the consensus committee, with p being much smaller than m. This blockchain architecture offers a promising solution to scalability challenges and can be widely applied across various applications. The proposed solution not only enhances efficiency but also demonstrates the ability to handle large volumes of transactions. Additionally, the likelihood of a malicious RSU being selected for the consensus committee is significantly reduced, ensuring a higher level of trust and security in the system.

2.2.5 Blockchain based federated Learning (FL) process and Proof-of-FL (PoFL) consensus mechanism for VANET

The authors of this paper [31] proposed a solution, to prevent broadcasting storm and ensure that the probability of receiving packets by the receivers do not fall. This solution is based on federated learning [32] and is blockchain-assisted [33]. Federated Learning(FL) is a machine learning based proposition which is distributed, where the vehicles gather data and train inde-

pendent machine learning models, which are called the local models. These models are then sent to the central aggregator. The aggregator creates a global model by averaging the local models. The created global model is then trained individually by all the mobile devices again to produce new local models that are updated. The updated local models are then sent to the aggregator and this process keeps on repeating until an appropriate result of the global model is attained.

There are mainly 3 stages in Blockchain based FL. The first stage includes data collection and the training of the local model, when a vehicle gathering data receives a Hello packet from another delegate vehicle, it waits for a random amount of time and then passes on this Hello packet along with the encrypted ID. The vehicles receiving this Hello packet for the first time will send an acknowledgement upon receiving it and this acknowledgement packet will consist of the encrypted ID of the forwarder. The second stage is a security check along with updating the FL Blockchain. The local models have to go through a security check done by the smart contract in the Federated Learning Blockchain. After passing the security check the local models are added to the FL Blockchain as microblocks. This security check uses a special algorithm known as Isolation Forest to detect any type of inconsistency. The announcement of new microblock addition is then broadcasted through the network the receiving vehicles will then change their individual copies of the FL Blockchain. Stage 3 is where aggregation of the local models is done by the RSUs. Whenever a vehicle would find an RSU in its proximity it will share the copy of the FL Blockchain it has. RSUs upon receiving a threshold number of microblocks then aggregate the Local models to produce Global models which are finally uploaded into Keyblocks. The entire process is repeated for a maximum threshold and this threshold is predefined by the Central Authority (CA).

During the Message dissemination phase, when an event takes place, the initiator generates an incident message. Vehicles that receive this message utilize the PoFL algorithm to calculate their score from the Global model. In this context, the score represents the number of acknowledgement packets received after the Hello packet is forwarded. To control the timing of events, a smart contract activates a timer, the duration of which is inversely proportional to the score of the vehicle nodes. The vehicle that reaches the end of its timer first proceeds to add a block to the message blockchain. This block contains the forwarded incident message, along with details such as location, time, and the concealed identity of the relay node. This approach ensures that the vehicle with the highest score becomes the relay node for the first hop, as it experiences the shortest waiting time. Subsequently, the remaining vehicles compete to become relay nodes for subsequent hops, continuing until the maximum number of hops is

reached.

The authors also proposed an incentive mechanism, where the model is composed of a Stackelberg game consisting of 2 stages. In the first stage the originator pays an incentive to the relay nodes for forwarding the message. In the second stage, the relay nodes pay an incentive to the vehicles who participated in federated learning forming the Global model of relay selection. The contributions of the vehicles are stored as permanent blocks with timestamps that cannot be modified, this is because the Federated Learning and the message dissemination processes are both based on blockchain. This method reduces time delay in consensus by 65.2% compared to other blockchain-based solutions. This also improves the message delivery rate by 8.2% and also performs much better in preserving the privacy of vehicles in the network. The FL process includes the usage of a smart contract that deals with malicious vehicles and prevents attacks. If a smart contract enforces a security check, lower Mean Squared Error (MSE) can be achieved using less number of iterations. This proposed method does not require sharing information such a s speed, direction of the vehicles unlike various other multi-hop relay selection approaches where beacon messages are used to do so which eventually becomes a threat to privacy. This approach preserves the privacy of vehicles, as to generate the dataset in blockchain and calculate relaying score in message dissemination only the direction and position of the sender vehicle are used, but even in these cases encryption is applied to keep the identities anonymous.

2.2.6 Voting based consensus algorithm with a price and reputation based incentive strategy for VANET

The authors of this paper [34] proposed a structured voting based consensus algorithm which is efficient and a new relay selection procedure along with an incentive mechanism based on a combined strategy scheme using both reputation and price. This integrated scheme encourages coordination and discovers any dishonest behavior in the network. The voting based consensus introduced here prevents broadcasting storms and properly selects relay nodes needed for forwarding the message.

Vehicles have to be registered with a central authority, prior to joining the blockchain network. They exchange beacon messages with each other frequently sharing vehicle information. When an event occurs , the vehicle associated with the event will create a transaction proposal. The vehicles having reputation more than the threshold value and have witnessed the accident/event will then broadcast their signature which is cryptographically encrypted. This signature acts as a portion of endorsement and vote for selecting the appropriate relay node in the first hop. For the voting needed for relay nodes, the vehicles calculate the Quality Factor

(QF) from the information it received through the beacons and decide its choice depending on the one that has the highest quality factor. The parameters needed for relay selection are stored in the blockchain so that the central authority can find out any type of malicious behavior for relay selection. If a predefined number of endorsements are obtained within a specific amount of time only then it becomes an endorsed message. The node that receives the highest number of votes will be chosen as the relay node. This node will forward the message and create a block. The voting based relay selection process and message forwarding will continue till a maximum hop number is reached or till the timer expires.

The incentive mechanism used is a combined one using both reputation and price. The originator has to pay an amount known as call compensation for causing the event. If a threshold number of endorsements is obtained by the originator for the transaction, before the timer runs out then the call compensation is split into the ratio w1:w2, for the endorser vehicles and the relay nodes. If a minimum number of endorsements is not obtained for a transaction then it is considered to be a fraud and the whole call compensation is given to the central authority as penalty. Any type of honest behavior for message dissemination causes the reputation of a vehicle to increase through receiving a reward and any type of malicious behavior means that either the originator creates a fake transaction proposal or the endorsers endorse a fake transaction proposal. It might also happen that a malicious relay node may not forward the message, in any case the reputation of the malicious vehicle would be decreased by the help of a penalty. Post consensus, the relay nodes create a block at every hop. The block keeps the record for all the parameters for reputation update, selection of relay nodes and the virtual credit transactions. All the vehicles in the network have individual copies of the blockchain which they keep on updating regularly.

For simulation the authors used OMNeT++ integrated with SUMO. The findings indicate that the suggested method can achieve an average time savings of 11% in message dissemination compared to alternative voting-based approaches. By integrating relay selection with consensus, the success rate of transmission can be enhanced by 17%. Moreover, the economic model, which combines price and reputation-based incentives, strengthens the system's resilience against collisions.

2.2.7 Blockchain-based IoV with the Byzantine Consensus Algorithm based on Time sequence and Gossip sequence (BCA-TG)

The authors of this paper [35] proposed IoV that is based on Blockchain and a Byzantine consensus algorithm based on Time sequence and Gossip protocol (BCA-TG). This proposed solution ensures the safety and security of the integrated network as it is decentralized and allows true authentication and trust computation. It is also very fault tolerant and efficient. The Iov nodes are split into roadside communication nodes (RCNs) and vehicle-mounted communication nodes (VCNs). The proposed architecture combines these 2 types of nodes to form a systematic blockchain cloud platform. Vehicle-mounted communication nodes (VCNs) are mobile nodes that are installed on mobile nodes i.e. vehicles and Roadside communication nodes (RCNs) are installed on fixed nodes i.e. roadside stations. Both the vehicles and the roadside base stations can send and receive information to and from the other nodes but only RCNs have storage capacities. Therefore, RCNs are chosen to be the consensus making node in this architecture. All the data in IoV is kept in the blockchain based cloud. Before creating a block the data produced by the RCN and VCN will have to win the RCN consensus and then it will get broadcasted.

The authors used the Gossip protocol for VCN and RCN communication and update. All the nodes in the network randomly communicate with each other, this eventually results in all the nodes having the same data. If there is any update in the information a node will forward it to its neighbors, however if there is no update in the information a node has then it will send an information update request to a neighboring node. This entire process will keep on repeating till all the nodes obtains the same updated information. Communication between nodes happens using the Push-Pull method. In the first part of this method, a node A will select a neighbor B in a random manner and then it will send an information update request to it. The neighbor node B will then send any information that the requester node A does not have. The requester A will then update its information and send the updated information to the neighbor node B. In the second part, the previously requester node A will send any information not present in its neighbor node B , B then updates its information and sends the updated information to A. The time required for both the nodes to have the same information is known as a cycle. The main advantage of this Push-Pull method is that both nodes obtain the same information in one cycle. A chronologically arranged series of data or information is known as a Time sequence. Only one type of information of objects is recorded by the unit time sequence at a time.Node time sequence is just a collection of 2D vectors that are arranged chronologically, and each of these vectors carries information on the nodes' entry and exit times within the network along

with any other information associated with it. A threshold is decided so that nodes cannot simultaneously enter and exit the network. In the event that the threshold for the number of nodes entering and departing the network is exceeded, the time window protection mechanism will automatically start up. As long as they are well within the threshold, the first n nodes in the node time sequence are the only ones that can join and leave the network; other nodes need to wait until the subsequent time window. The Push-Pull communication process produces 3 kinds of information, namely Local Information (LI), Consensus Information (CI) and Update Information (UI). The RCNs of the IoV network engage in the consensus mechanism. In the beginning 2 RCNs are chosen to be the consensus makers and both of them derive their update information from their local information. They then communicate with each other using the Push-Pull method and update their UI. The information of the next pair of RCNs will be updated using this updated UI. This entire process keeps on repeating until all the nodes in the network have the same update information, Finally from the last updated UI the Consensus Information is derived.

The proposed improved Byzantine Consensus Algorithm is used for IoV authentication, this algorithm consists of 6 steps. It will initially determine whether nodes enter or leave the network. When they enter and exit, the node entry/exit method is carried out using a time sequence, after which the nodes are output. If the information was created by an RCN, it would be announced by the RCN in the second step; otherwise, it would be submitted to an RCN for announcement. The third phase involves broadcasting the information to all network nodes engaged in consensus. The nodes then exchange information by interacting with one another via the Push-Pull method and the Gossip protocol, using the most recent updated node UI. In the next step, it is checked if the Consensus information is reached if yes then the CI is confirmed against the initial info. Finally the consensus output is stored in the blockchain as a block and it is sent to all the VCNs and RCNs.

The BCA-TG algorithm offers decentralization because information in the network can be verified without the aid of a central authority, byzantine fault tolerance because efficiency is maintained, and consensus can be reached even if there are fewer than half as many Byzantine nodes as other nodes in the network, and Scalability as the nodes in the Iov network can communicate with each other even if multiple nodes enter and exit the network.

2.3 Summary

VANET or Vehicular Ad-Hoc Network is an application of MANET or Mobile Ad-Hoc Network. It faces various types of challenges when implemented in real life which includes the areas such as security and privacy, reliable routing, communication and connectivity, authentication and many more. Blockchain is one of the probable solutions which can be used to tackle these difficulties. Blockchain has features such as immutability, privacy, transparency, decentralization, security etc. Consensus mechanisms of blockchain can be used to validate the messages and identities of the nodes in VANET. It prevents unauthorized access to the network. Blockchain has huge potentials to be used in VANET and solve the issues to be further implemented in real life.

PoW is highly secure against various attacks, but it is highly time and energy-consuming as it needs to solve a hard mathematical puzzle to be selected as a miner, making it inefficient to use in VANET. PBFT is fault-tolerant and the most suitable one to be used in VANET, but when the number of nodes increases PBFT fails to perform as expected. PoQF gives more correct validations and is also faster due to its voting based validation system, but it is vulnerable to malicious nodes if they compose more than 50% of the mining group. POVS-BFT reduces the complexity of the system by reducing the consensus committee size, but it can face an attack if an insider malicious RSU is selected to be in the consensus committee. PoFL is obviously a faster approach since it results in a greater number of uploaded local models within a given time compared to a solution without blockchain. However, its dependency on the aggregator raises integrity and security issues. An incentive mechanism based on both price and reputation makes the system stronger against collusion attacks. The voting-based consensus protocol, along with the quality factor associated with each of the nodes, results in impressive performance. However, it has the risk of failing when there is a greater number of malicious nodes. BCA-TG has advantages such as decentralization, Byzantine fault tolerance, and scalability. However, the communication complexity and the need for nodes to reach agreement through the gossip protocol may become more resource-intensive and less practical in highly decentralized and large-scale IoV systems.

Altogether we can say blockchain can solve many of the critical issues faced in VANETs but it requires specializations to improve the performance of the system and it is an open field for research.

Chapter 3

Proposed Solution

In this chapter, we first provide background information on the topic. Next, we discuss the problem we aimed to solve and the motivation behind our proposed mechanisms. We then explain the system model and assumptions, followed by the description of the proposed Consensus Mechanism, Message Dissemination Process, and Incentive Mechanism.

3.1 Background

VANET has dynamically changing topology due to the moving vehicles which act as the wireless nodes in the network. The message dissemination process is thus one of the most critical aspects of VANET. In this case Blockchain is a suitable solution due its efficient message validation and dissemination capability. The existing consensus mechanisms such as Proof-of-Work (PoW) has high computational cost and long propagation delay [6], Proof-of-Stake (PoS) is biased towards nodes with higher stakes [7], [8] etc. The Practical Byzantine Fault Tolerant (PBFT) consensus algorithm is the most suitable for VANETs due its tolerance to malicious nodes [12]. But PBFT fails in case of a large number of nodes, which is exactly the case in VANET. A hybrid of PoW and PBFT can serve the requirements of VANET in the best manner. The selection of relay nodes to forward the message is another crucial issue as inefficient selection may cause broadcast storm and unavoidable latency. Forwarder nodes must be selected so that they can cover a larger distance. Nodes should get incentives to encourage honest behaviour and they should get penalty to discourage malicious behaviour.

3.2 Problem Statement

One of the major challenges in VANET is to ensure minimum latency in the message validation and message dissemination process. It is not of great use to know about the incident after already taking the direction of the place where the incident took place or even worse after reaching that place. Thus to ensure maximum road safety, the message validation and dissemination process must be very fast.

One of the solutions for making the message validation process faster includes voting. Here the neighbor vehicles broadcast their votes to other neighbor vehicles, so that all those vehicles can come to the same validation result after proper calculation. This process may lead to a broadcast storm which degrades the quality of the entire network significantly and does not allow the system to work as expected. To avoid this communication overhead, there must be the least amount of messages passing in the network. The calculation for validation may itself require significant computational power. This aspect must be taken into consideration as well.

For the message dissemination process the system needs to choose forwarder nodes at each hop level. The algorithms sometimes follow a rigorous calculation to select the best one. The calculation itself sometimes can be very much time consuming. While choosing the forwarder nodes many parameters can be used for best results such as the number of vehicles it can reach, the rate of successful transmissions and so more. Now if the parameters become expensive to compute then it will not matter even if they provide better selection. The parameters can even be biased and produce biased results. We need to select a relay node that can cover the maximum possible distance in the minimum possible time, using the minimum number of broadcast messages. To be efficient we should be able to minimize the overlapping of covered areas.

Our focus is to give an efficient consensus algorithm along with a message dissemination process and an incentive mechanism which results in minimum validation and dissemination latency, at the same time avoids broadcast storms.

3.3 Motivation

Proof-of-Work (PoW) and Practical Byzantine Fault Tolerant (PBFT) are two of the most prominent consensus mechanisms for blockchain. PoW has high computational cost and latency while PBFT is not suitable in networks where the number of nodes is high. One of the major challenges of VANET is that the network is very short lived, due to high mobility of the vehicles. To overcome this challange, the process of message validation must be both accurate and fast. PoW and PBFT cannot be implemented in VANET in their basic form. The huge number of messages being passed in the mechanisms can lead to broadcasting storms and network congestion. We propose an efficient consensus mechanism for blockchain based VANETs that can mitigate the issues in PoW and PBFT. Our goal is to make the consensus mechanism less costly in terms of the number of messages passed. Reducing the number of messages passed is a big challenge, as insufficient information can cause inaccurate calculations. We take advantage of both PoW and PBFT to create a hybrid consensus mechanism that is efficient to use in

blockchain based VANETs.

Message dissemination process must choose relay nodes wisely so that the message can reach the maximum amount of vehicles, cover the maximum distance within the shortest possible time, using the minimum possible broadcasts. In [29] the authors proposed a mechanism that takes help from probability to assess channel quality between the sender and receiver during the selection process. Based on this they proposed a Quality Factor to choose the best relay node. Between the two components of the quality factor one is always strictly larger than the other and hence always the dominating one. It may give us biased results. The system doesn't tell us in which direction we have to select the relay node. There is always a higher possibility of overlapping of covered areas and also a higher possibility that an area is not covered at all. Another important issue is that we must give more focus on disseminating the message to the farthest possible distance rather than to a certain hop level. In case of a congested network, disseminating upto a certain hop level may restrict the dissemination to longer distance. It may fail to reach vehicles which are at distant and give poor performance results.

Incentive mechanisms are needed to encourage participation of the veicles in the network and honest behaviour from them. It is also needed to discourage the malicious behaviour of nodes. In our proposed incentive mechanism we not only considered monetary units but also reputation of the vehicles. Using only monetary units may not always ensure honest behaviour from vehicles who have no need of it anymore. Reputation is needed anyway to function in the process of the network. We have also incorporated this reputation in the validation process to increase its importance to the vehicles.

3.4 System Model and Assumptions

In this section we present the system scenario and assumptions for our proposed solution. We consider two types of edge devices: *vehicles* or mobile edge nodes and *RSUs* or edge computing servers. We assume the use of Dedicated short-range communication (DSRC) protocol for the wireless communication among vehicles and RSUs. As the communication range for DSRC is over 1km, we assume the same in this scenario. Each node must register with the regulatory authority prior to joining the vehicular network and obtain the required identifiers, such as a wallet address and a set of public and private keys for communications that are private. V2I communication is a viable option for this communication. Using edge caching, each appends its copy of the blockchain, as explained in [36]. The regulatory body keeps track of the expiration of inactive keys to stop attacks that can be launched from a distance using outdated accounts [37]. We use a blockchain called the *incident chain* which contains all the information related to an

incident including the incident message and its validity, the list of voter vehicles along with necessary information of each of them such as, vote given by the vehicle on the validity of the message, its reputation and incentive and so on. The vehicles periodically send beacon messages to each other, giving the basic information about themselves such as their location, speed etc. From the received beacon messages the vehicles maintains a neighbor list of their own.

3.5 Consensus Mechanism

When an event occurs, the originator associated with the incident initiates an incident message with the details of the incident. The message is then broadcasted to the neighbors of the originator. A vehicle is considered as a neighbor if it is found inside half of the transmission range of the originator. Transmission range is the farthest distance between any two nodes at which a signal from one node might directly reach the other with adequate intensity to accurately decode the encoded information. Thus, the motive behind considering neighbors in this way is to ensure the quality of the transmitted message in every direction.

After receiving the incident message, only the selected neighbor vehicles according to the descending order of their reputation will broadcast their vote on the validity of the incident message. The first reason behind introducing selective voting system is to reduce the number of message passing and mitigate the chances of traffic congestion created by the broadcasted vote messages. The second reason is to avoid malicious nodes at an earlier stage by only considering highly reputed vehicles. Limiting the number of voters has some challenges. If the algorithm ends up with a very small number of voters and votes, then it has to take decision only based on few information and votes it has. The validation may not be generalized in this case. If the algorithm ends up with a large number of voters, then the malicious and less reputed voters may also get selected and the result will get corrupted. In this case the process may introduce unacceptable latency. There should be a balance. To introduce this balance our proposal includes two conditions that a vehicle needs to fulfill in order to broadcast its vote. The first one is, a vehicle has to be a neighbor of the originator which means it must be located inside half of the transmission range of the originator. The second condition is, it must have the highest reputation at that moment among all the neighbor vehicles who have not voted yet. The second condition is implemented by controlling the contention window size in the backoff strategy of the underlying protocol according to the reputation of the vehicle. If the vehicle has a high reputation then the size of the contention window is smaller. Hence, it is able to broadcast its vote sooner than others. Following this strategy the neighbor vehicles

will broadcast their votes in the descending order of their reputation values. The conditions ensure quality of the transmitted message and trust worthiness of the vehicle, respectively.

Upon receiving votes from other vehicles, each of the voter vehicles starts calculating the weighted sum of votes. The process of calculating the weighted sum of votes is that, when a particular vehicle receives a broadcasted vote message from another voter vehicle i, it immediately fetches the reputation of that vehicle. At first, it tries to fetch the reputation from its own neighbor list. If its not in the list then the vehicle fetches the reputation from the blockchain. Now it calculates the weighted vote Wv_i where, weight for the vote depends on the reputation R_i of the voter vehicle i. The vote of a highly reputed vehicle has more weight than the vote of a vehicle with lower reputation. As a result, a vehicle with higher reputation makes a larger contribution to the weighted sum than a vehicle with less reputation. This ensures more engagement of higher reputed vehicles than that of lower reputed vehicles in the message validation process. The vehicle keeps summing the weighted votes as it receives votes from other voter vehicles until threshold number of votes W is achieved where W is predefined or t seconds have passed where t is also predefined. The weighted sum of votes Wv, is calculated following the equation given below:

$$Wv = Wv_1 + Wv_2 + Wv_3 + ...Wv_n, Wv \geq W \tag{3.1}$$

From the total weighted votes it considers whether at least a threshold, p percentage of the votes are true or not. If it is, then the message is validated by the vehicle as true, otherwise the message is false. The reason for introducing weighted sum of votes is to make the validation process faster. The process calculates the sum dynamically while receiving the votes and stops as soon as it reaches the predefined threshold level. It prioritizes the votes of highly reputed voters over others. The process does not need to wait for all the voters to vote. It limits the amount of considered votes. It does not require any extra calculation time. It is a 'on the go' process which makes the validation much faster with less calculation.

After the message validation process, the vehicle creates a block with the information of the incident, the resulting validity of the incident message (valid or invalid), the votes and other related information of the voters. The vehicle waits a certain amount of time which is proportional to $1/reputation$, to ensure higher reputed vehicles get priority. After the waiting period, it adds the block in the blockchain if no block is added for this incident or the added block contains incorrect information. Other neighbors then check the correctness of the added block. If any of them finds erroneous information in that block, it adds the block which was created by it after completing the validation process, generating a fork to the blockchain. The

branch containing the block with all correct information is finally accepted by the legitimate neighbors and becomes the main branch of the blockchain. Other branches with erroneous blocks get discarded. The process ensures blocks are added for both valid and invalid incident messages, along with the information of the voters. The information of the voters is stored to distribute the incentives based on their behaviour (legitimate or malicious). The reputation of the vehicles stored in the blockchain are also used in the validation process. Moreover the blockchain system ensures easy access to the information by the vehicles.

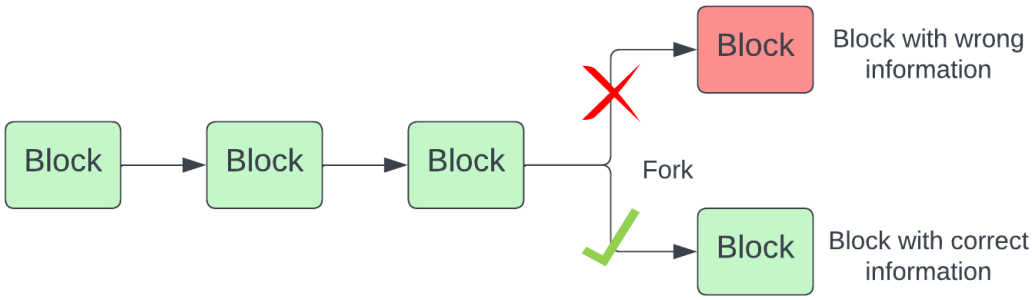

Figure 3.1: Resolving fork in the blockchain.

Malicious behaviour from the nodes can be very fatal to the system. Malicious behaviour of the voters may result in incorrect validation of the incident message. To tackle the situation, the vehicles that have voted against the agreed upon validity of the incident message get penalty in terms of incentives. Steps are taken to tackle malicious behaviour from the miner vehicles as well. The vehicle which adds the block of the accepted branch gets reward in terms of incentive for mining the block with correct information. The vehicles that add block with false information get penalty for their malicious behaviour. They lose the permission to add any block in the blockchain for the next n incidents along with penalty in terms of incentive. Thus the system successfully discourages any malicious behaviour from voters and miners.

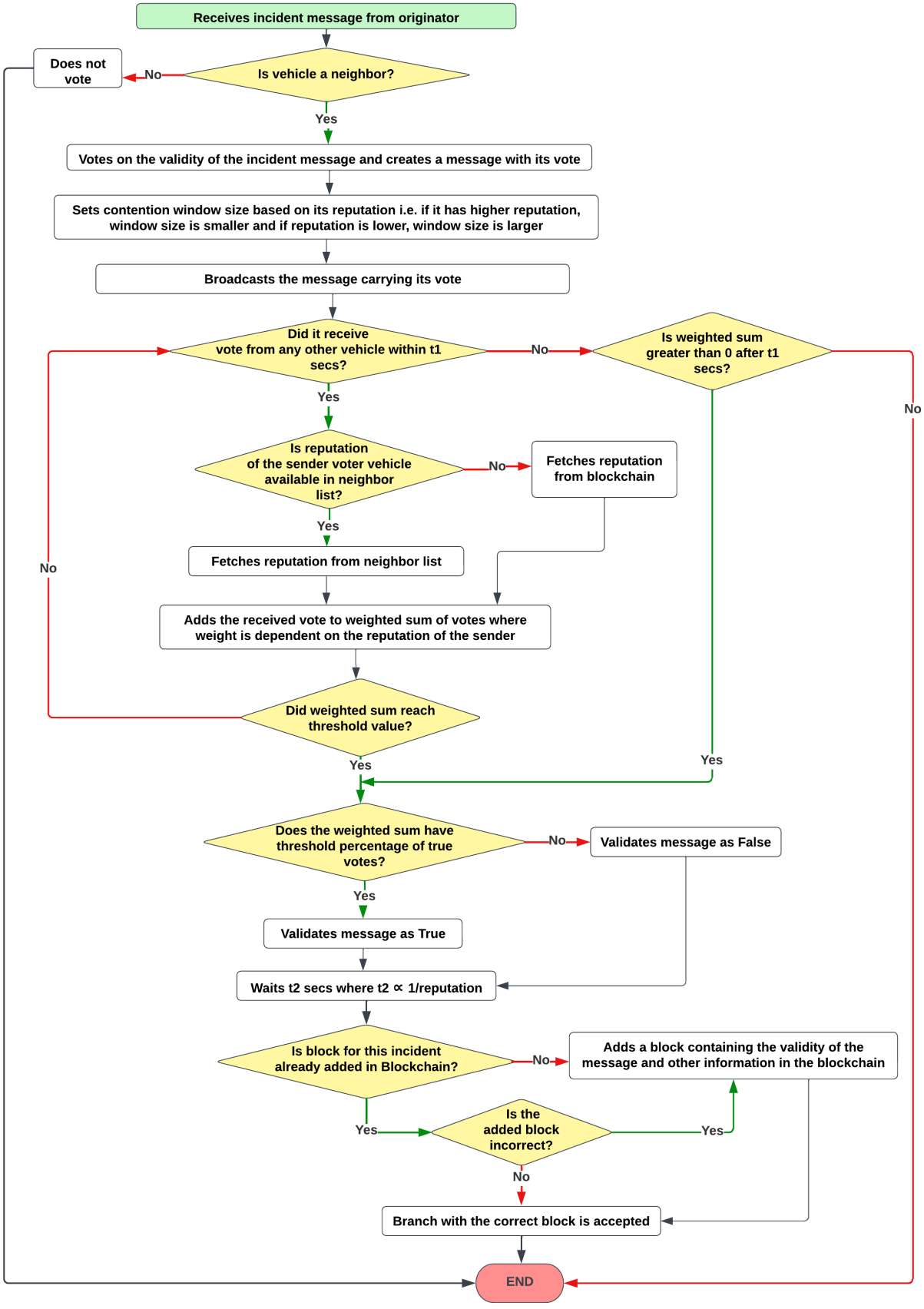

Figure 3.2: Actions taken upon receiving an incident message by a vehicle.

3.6 Message Dissemination Process

After the message validation and block mining process, the system must start the message dissemination process. If the message is validated as true then the first hop level forwarders are selected and the message is forwarded to its neighbours. For the selection, we propose three conditions that need to be fulfilled by a vehicle to be selected as a forwarder node.

- The first one is, the vehicle has to be a neighbour of the miner that is it has to reside inside half of the transmission range of the miner vehicle. It ensures that the vehicle received an uninterrupted message from the previous level forwarder.
- The second condition is that, the node has to be in front of the miner. It is because the vehicles that are behind it are supposed to have already received the broadcasted incident message by the previous level forwarder.
- The third condition is that the node has to be at the maximum distance from the miner. It can be ensured using the location information in the beacon messages broadcasted by the vehicles. The third condition ensures that the message is disseminated to the longest possible distance using the smallest number of forwarders. It also guarantees the minimization of the total number of broadcast messages in the mechanism.

A vehicle that satisfies all of these three conditions are selected as a forwarder node to broadcast the message to its neighbours at the next hop level. Two forwarders in a two-way street and four forwarders in a junction for each direction is chosen in the same manner. The forwarder nodes then broadcast the message to their respective neighbor nodes and the next hop level forwarder nodes are chosen following the same process from neighbor vehicles moving behind in the same direction.

The forwarder node selection and message forwarding process continues repetitively until a certain distance is covered. The threshold value for the distance to be covered ensures that the message is disseminated to the distant vehicles both in dense and sparse networks, unlike the case when the message is disseminated until a threshold number of hop levels are crossed. It is because in congested networks the maximum hop level can be reached covering a smaller distance than expected. Thus the maximum distance constraint results in better performance in this respect.

3.7 Incentive Mechanism

An incentive mechanism based on both price and reputation makes the system stronger against collusion attacks as mentioned in [34]. Thus we propose an incentive mechanism where the actions of the vehicles affect both their reputation and monetary savings.

- **Reputation:** Once a block containing the correct information of a validated incident is added in the incident blockchain, following events occur:
  - The reputation of the miner vehicle node that has mined the block with all correct information, is increased.
  - The reputation of the honest voter vehicles are increased and the reputation of the dishonest voter vehicles are decreased as per the agreed upon validation of the message.

  If α is the coefficient factor here then,
  Increase in reputation of vehicle i:

  $$R_i = R_i + \alpha R_i, [0 \leq \alpha \leq 1] \tag{3.2}$$

  Decrease in reputation of vehicle i:

  $$R_i = R_i - \alpha R_i, [0 \leq \alpha \leq 1] \tag{3.3}$$

- **Monetary Units:** Monetary incentive is charged from several entities. The incident originator is charged, as a compensation for causing the incident. The dishonest miner vehicles are also charged for mining block with incorrect information. Altogether it is called Originator, Miner Compensation, OMC. After the entire validation process of the message, the compensation is distributed as follows:
  - The honest miner vehicle will get a part of OMC called OMC_{mn}.
  - The other part of OMC will be distributed among the honest voters called OMC_{vt}. So each of the honest voters will get OMC_{vt}/n, where n is the total number of honest voter vehicles.

  After the message validation process, an amount of monetary incentive is also charged from the dishonest voter vehicles as compensation for being dishonest in voting called Dishonest Compensation, DC. If the message is validated as true then DC is distributed among the forwarder nodes. So each forwarder vehicle will get DC/m, where m is the total number of forwarder vehicles.

If the message is validated as false then the message will not be forwarded and thus DC and OMC are distributed among the honest voters and the honest miner only.

3.8 Summary

We propose an efficient consensus mechanism for blockchain-based Vehicular Ad-Hoc Networks (VANETs) to improve message validation and dissemination processes. The existing consensus mechanisms in blockchain are not suitable to be used in VANET in their basic forms. So we take advantage of the best features of the existing consensus mechanisms Proof-of-Work (PoW) and Practical Byzantine Fault Tolerant (PBFT) to make a hybrid better one. The system model assumes two types of edge devices, vehicles, and edge computing servers, using the DSRC protocol for communication. The proposed mechanism reduces communication overhead and broadcast storms while considering the reputation of vehicles. It introduces selective voting and weighted voting to accelerate the validation process. Additionally, it outlines a message dissemination process based on forwarder node selection to cover maximum distance with minimum broadcast messages. An incentive mechanism incorporating reputation and monetary incentives is also suggested to encourage honest behavior and discourage malicious activities.

Chapter 4

Result Analysis

In this Chapter we analyse the simulation results of the proposed consensus mechanism. At first, we discuss the Simulation Environment for the study then the Performance Metrics we have used. In the following four sections we have compared the number of messages passed with and without considering reputation in the consensus mechanism, we have showed the result accuracy level with respect to different values of threshold for weighted sum of vote, we have also compared true positive and false positive validation with respect to threshold for weighted sum of votes and finally we showed the result accuracy with respect to threshold for true votes.

4.1 Simulation Environment

The simulation environment for this study utilizes the OMNet++ platform in conjunction with SUMO (Simulation for Urban Mobility). By integrating these tools, a comprehensive simulation framework is created to analyze the proposed consensus mechanism for Vehicular Ad-Hoc Networks (VANETs). In the simulation, a total of 48 neighbor vehicles are considered, representing a realistic scenario where vehicles interact with their immediate surroundings. The reputations of these vehicles are assigned values within the range of 10 to 40, reflecting the varying levels of trustworthiness and reliability among the vehicles in the network. This simulation environment enables the evaluation and assessment of the consensus mechanism's performance and effectiveness in a controlled and representative setting, providing valuable insights into its potential real-world implications.

4.2 Performance Metrics

The simulation metrics employed in this study focus on evaluating the performance of our proposed blockchain architecture in Vehicular Ad-Hoc Networks (VANETs). The first metric involves comparing the number of messages passed with and without considering reputation. This analysis provides insights into the impact of reputation-based voting on the overall communication overhead within the network. Another important metric is the result accuracy with

respect to the threshold for the weighted sum of votes. By varying the threshold, the study examines how accurately the consensus mechanism aligns with the desired outcome. Additionally, the comparison of true positive and false positive validations, considering different thresholds for the weighted sum of votes, allows for an assessment of the mechanism's ability to validate results correctly while minimizing false positives. Lastly, the result accuracy is evaluated concerning the threshold for true votes, which offers insights into the mechanism's accuracy when considering only the trustworthy votes. These simulation metrics provide a comprehensive understanding of the system's performance, shedding light on its impact on network communication, result accuracy, and validation in the context of Vehicular Ad-Hoc Networks.

4.3 Comparison of the number of messages passed with and without considering reputation

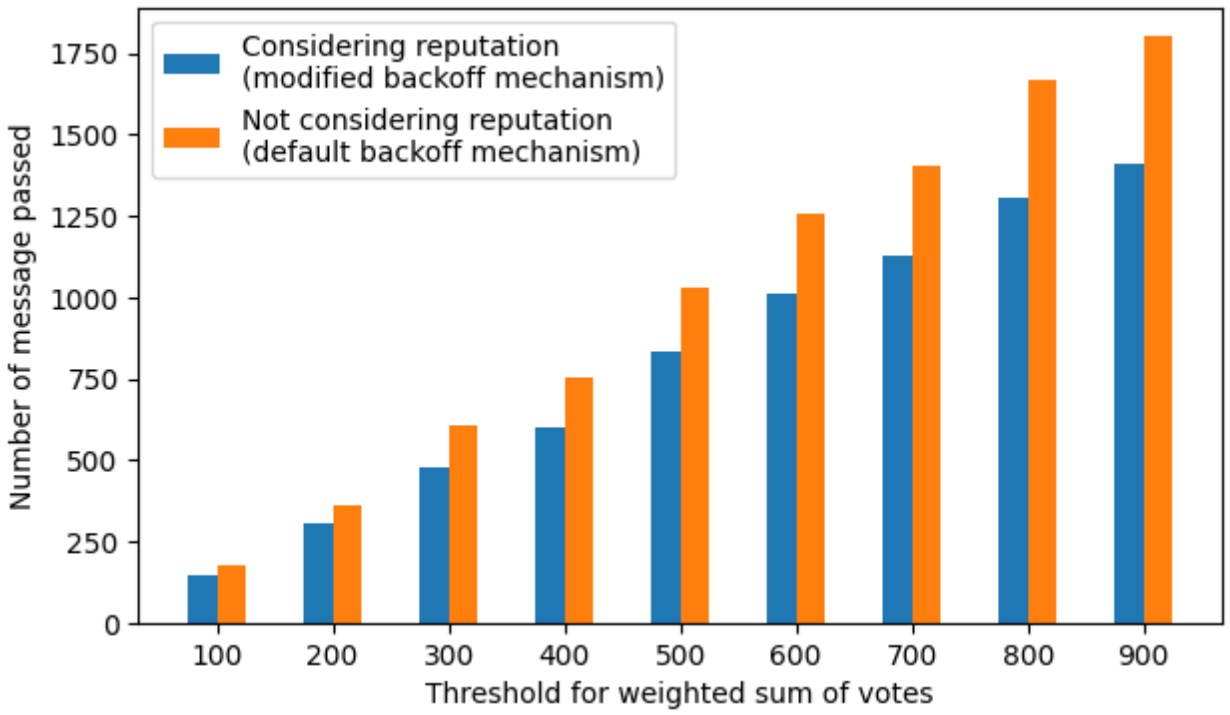

Figure 4.1: Comparison of the number of messages passed with and without considering reputation

Figure4.1 shows the number of messages passed with respect to the threshold for weighted sum of votes W, in our proposed consensus mechanism in two scenarios. One is when the weighted sum of votes is calculated considering the reputation of the voter vehicles. Other is when the reputation of the voter vehicles is not considered. When the reputation is considered, the modified backoff mechanism is used which results in broadcasting the votes in the descending

order of vehicle reputation values. When calculating the weighted sum of votes, the weight of a vote is proportional to the reputation of that specific voter. The way votes are being broadcasted, they arrive in the descending order of their weights as well. Thus in this case the weighted sum of votes is achieved with the least amount of votes possible, resulting in the least number of messages broadcasting. On the other hand, when the reputation is not considered, the default backoff mechanism is used. The votes are not broadcasted in any specific order. Thus it may require more votes to achieve the threshold weighted sum of votes W, resulting in higher number of messages passing. The difference in the number of messages passed is significant when the threshold for weighted sum of votes W is higher. Consequently, we can say the difference of the number of messages passed will be even higher with the case when weighted sum of votes is not used and all the messages have to be broadcasted. So in this respect, our proposed mechanism performs significantly well.

4.4 Result accuracy with respect to threshold for weighted sum of votes

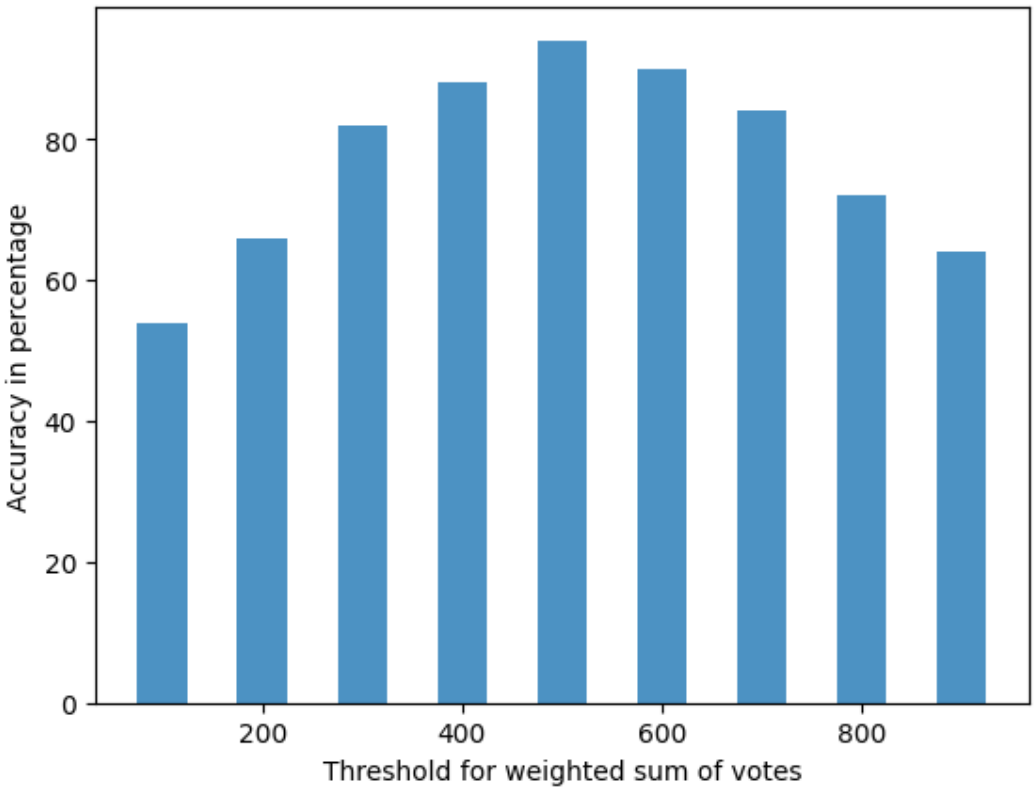

Figure 4.2: Result accuracy with respect to threshold for weighted sum of votes

Figure4.2 shows the average result accuracy level with respect to the threshold for weighted

sum of votes W in our proposed consensus mechanism. When the threshold for weighted sum of votes W is lower, the mechanism can reach the weighted sum of votes considering lower number of votes. It then validates the message only based on those inadequate amount of votes. In this case, it may happen that only some votes from very highly reputed vehicles are considered. The few amount of voters can then monopolize the system. Thus some messages may not be validated correctly because not enough amount of different voters are considered. As the threshold value W increases, the number of considered votes increases and thus the accuracy increases as well. On the other hand, when the threshold for weighted sum of votes W is higher, the mechanism needs to consider a larger number of votes to reach the threshold. In this case, the votes of the malicious vehicles or the vehicles with lower reputation levels may also get considered. Thus the validation process may fail to validate correctly because of those votes from malicious voters. The accuracy level decreases again. So a threshold value for weighted sum of votes W in the mid range gives the best results. For our case it is 500-600.

4.5 Comparison of the true positive and false positive validation with respect to threshold for weighted sum of votes

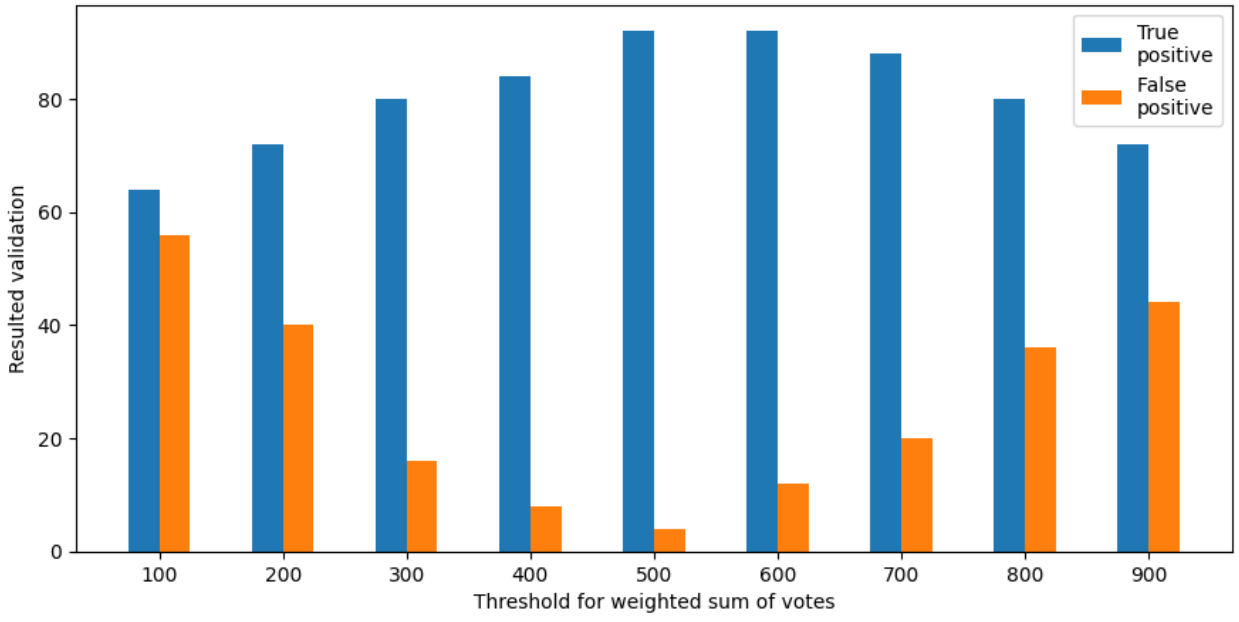

Figure 4.3: Comparison of the true positive and false positive validation with respect to threshold for weighted sum of votes

Figure4.3 shows the average level of resulted true-positive and false-positive validations in our proposed consensus mechanism with respect to the threshold for weighted sum of votes W.

As we have seen in figure4.2, when the threshold W is at lower value the accuracy is lower. Consequently the rate of true messages validated as true or the true-positive level is lower as well. As the accuracy is lower the rate of false messages validated as false is also lower, resulting in a higher rate of false messages validated as true. Thus the false-positive rate is higher. But false-positive rate doesnt exceed the rate of true-positive. It is because when the threshold for weighted sum of votes is lower, the mechanism considers the few votes from the highly reputed vehicles only. They are less likely to behave maliciously and vote against the actual validity of the message. As the threshold W increases, the accuracy level increases. Thus the rate of true-positive increases and the rate of false-positive decreases. When the threshold value is even higher, the accuracy decreases, the true-positive rate decreases and the false-positive rate increases. But the increase is slow in false-positive rate. It is because the system considers votes in descending order of the voters' reputations. Thus even though the system takes a larger amount of votes, the votes of the malicious voters are likely to get selected after all the highly reputed and honest voters are already selected. So again a threshold value for weighted sum of votes W in the mid range gives the best results.

4.6 Result accuracy with respect to threshold for true votes

Figure4.4 shows the average result accuracy level with respect to the threshold of true votes p to consider a message as true. It means if $p\%$ of the weighted sum of votes W_v is true then the message is validated as true otherwise its validated as false. As we can see in the figure when threshold of true votes p is low, the accuracy is low. It is because when p is less, many false messages can reach this low threshold easily and validate as true. As p increases, the accuracy increases. It is because now the messages have to get a considerable amount of true votes to be validated as true. It is not as easy as before. When the value of p is even higher the accuracy decreases. It is because now that the messages have to get a higher amount of true votes, which is difficult to achieve. Thus many true messages may be validated as false. Thus a threshold value for true votes p in the mid range gives the best results. For our case it is 40-60.

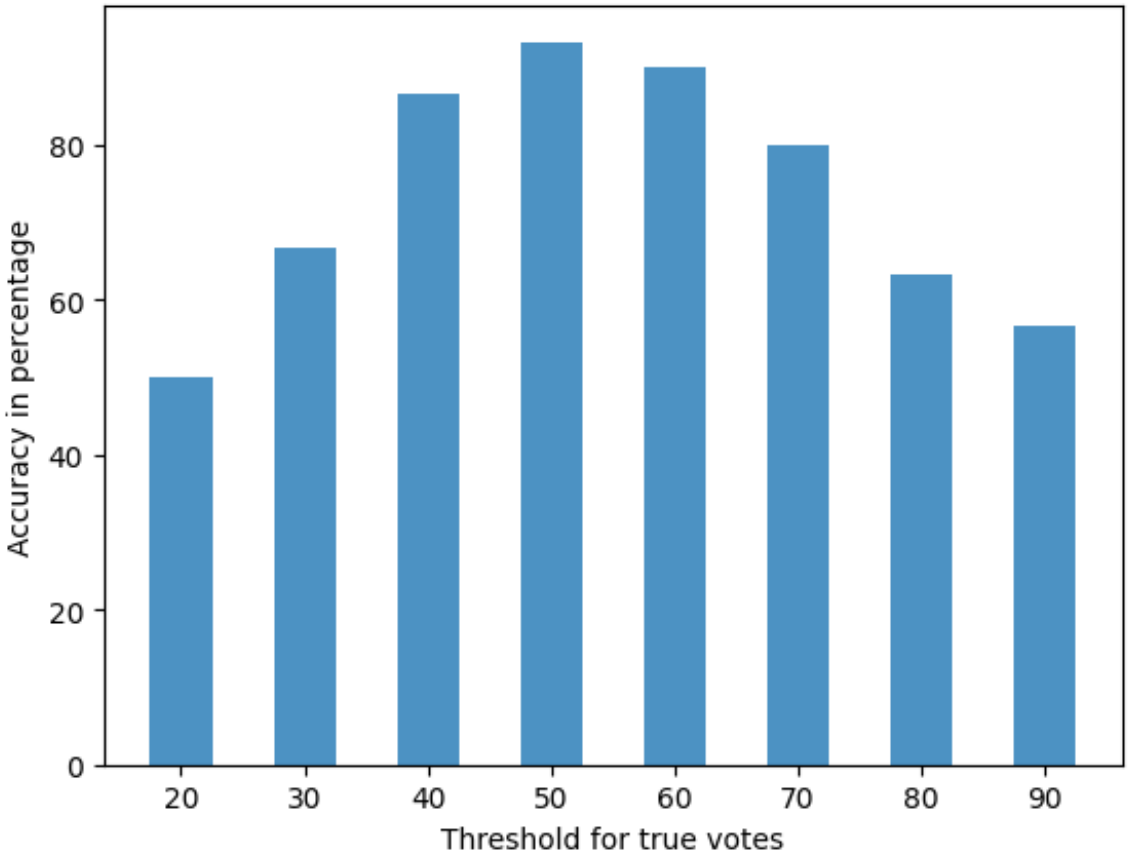

Figure 4.4: Result accuracy with respect to threshold for true votes

Chapter 5

Conclusion and Future Work

The main objective of our thesis is to employ Blockchain technology in VANET with an efficient consensus mechanism, message dissemination mechanism and incentive mechanism to address some of the fundamental issues in VANET, such as broadcast storms and increased message validation and dissemination latency. Nowadays the implementation of blockchain in VANETs is sky rocketing due to its unique set of services. We have included some of the most important relevant works in this area. In the light of the researches done so far, we propose a new consensus mechanism that is a hybrid of the best practices of common existing consensus mechanisms PoW and PBFT. We propose to use selective voting system with the help of weighted sum of votes. It reduces cost of the system as it reduces the number of message passing, while achieving high accuracy level. Thus the entire validation process becomes faster and cheaper. We also present a message dissemination process which will be able to pass the true validated message taking the least possible time and least possible number of broadcast messages. We propose an incentive mechanism that will encourage the participants to behave honestly. The simulation is done in omnet++ and the necessary results are analyzed to support our claim. In our specific environment our simulations results show higher accuracy when the threshold for weighted sum of votes is between 500-600 and threshold for true votes is between 40-60.

In future we expect to work more intensively on the incentive mechanism as it has great influence on the accuracy of the system. Specifically we expect to improve the reputation system. There are few works which are done on how a vehicle will choose its vote towards an incident message. So we expect to work on the voting mechanism as well.

Bibliography

[1] Zanjireh, M.M. and Larijani, H., 2015, May. A survey on centralised and distributed clustering routing algorithms for WSNs. In 2015 IEEE 81st Vehicular Technology Conference (VTC Spring) (pp. 1-6). IEEE.

[2] Rahman, A.U., Malik, A.W., Sati, V., Chopra, A. and Ravana, S.D., 2020. Context-aware opportunistic computing in vehicle-to-vehicle networks. Vehicular Communications, 24, p.100236.

[3] Gazdar, T., Belghith, A. and Abutair, H., 2017. An enhanced distributed trust computing protocol for VANETs. IEEE Access, 6, pp.380-392.

[4] Kim, S., 2019. Impacts of mobility on performance of blockchain in VANET. IEEE Access, 7, pp.68646-68655.

[5] Saravanan, M. and Ganeshkumar, P., 2020. Routing using reinforcement learning in vehicular ad hoc networks. Computational Intelligence, 36(2), pp.682-697.

[6] Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S. and Danezis, G., 2019, October. SoK: Consensus in the age of blockchains. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies (pp. 183-198).

[7] Kang, J., Xiong, Z., Niyato, D., Ye, D., Kim, D.I. and Zhao, J., 2019. Toward secure blockchain-enabled internet of vehicles: Optimizing consensus management using reputation and contract theory. IEEE Transactions on Vehicular Technology, 68(3), pp.2906-2920.

[8] Yang, Zhe, et al. "Blockchain-based decentralized trust management in vehicular networks." IEEE internet of things journal 6.2 (2018): 1495-1505.

[9] Chen, L., Xu, L., Shah, N., Gao, Z., Lu, Y. and Shi, W., 2017. On security analysis of proof-of-elapsed-time (poet). In Stabilization, Safety, and Security of Distributed Systems: 19th International Symposium, SSS 2017, Boston, MA, USA, November 5–8, 2017, Proceedings 19 (pp. 282-297). Springer International Publishing.

[10] Cebe, M., Erdin, E., Akkaya, K., Aksu, H. and Uluagac, S., 2018. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE communications magazine, 56(10), pp.50-57.

[11] Zhang, L., Luo, M., Li, J., Au, M.H., Choo, K.K.R., Chen, T. and Tian, S., 2019. Blockchain based secure data sharing system for Internet of vehicles: A position paper. Vehicular Communications, 16, pp.85-93.

[12] Choi, B., Sohn, J.Y., Han, D.J. and Moon, J., 2019, July. Scalable network-coded PBFT consensus algorithm. In 2019 IEEE International Symposium on Information Theory (ISIT) (pp. 857-861). IEEE.

[13] Khan, Adnan Shahid, et al. "Secure trust-based blockchain architecture to prevent attacks in VANET." Sensors 19.22 (2019): 4954.

[14] M. W. Maier, D. Emery, and R. Hilliard, "Software architecture: introducing IEEE standard 1471," Computer, vol. 34, no. 4, pp. 107–109, 2001.

[15] M. W. Maier, D. Emery, and R. Hilliard, "ANSI/IEEE 1471 and systems engineering," Systems Engineering, vol. 7, no. 3, pp. 257– 270, 2004.

[16] D. Emery and R. Hilliard, "Every architecture description needs a framework: expressing architecture frameworks using ISO/IEC 42010," in Proceedings of the Joint Working IEEE/IFIP Conference on Software Architecture & European Conference on Software Architecture (WICSA/ECSA '09), pp. 31–40, Cambridge, UK, September 2009.

[17] T. Kosch, C. Schroth, M. Strassberger, and M. Bechler, Automotive Internetworking, Wiey, New York, NY, USA, 2012.

[18] https://www.extremetech.com/extreme/176093-v2v-what-arevehicle-to-vehicle-communications-and-how-does -it-work"V2V: What are vehicle-to-vehicle communications and how do they work?", Accessed: 21-06-2015.

[19] http://www.ijlera.com/papers/v2-i4/part-II/43.201704190.pdf

[20] Singh, M.; Kim, S. Introduce reward-based intelligent vehicles communication using blockchain. In Proceedings of the 2017 International SoC Design Conference (ISOCC), Seoul, Korea, 5–8 November 2017; pp. 15–16.

[21] Dorri, A. BlockChain: A Distributed Solution to Automotive Security and Privacy. IEEE Commun. Mag. 2017, 55, 119–125.

[22] Joy, J.; Gerla, M. Internet of Vehicles and Autonomous Connected Car–Privacy and Security Issues. In Proceedings of the 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017; pp. 1–9.

[23] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." Decentralized business review (2008): 21260.

[24] Castro, Miguel, and Barbara Liskov. "Practical byzantine fault tolerance." OsDI. Vol. 99. No. 1999. 1999.

[25] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. Mccorry, S. Meiklejohn, and G. Danezis, "SoK: Consensus in the Age of Blockchains," Proc. of the 1st ACM Conference on Advances in Financial Technologies, Zurich, Switzerland, Oct. 2019.

[26] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward Secure Blockchain-Enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory," IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 2906-2920, Mar. 2019.

[27] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain based Decentralized Trust Management in Vehicular Networks," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1495-1505, Apr. 2019.

[28] L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, and W. Shi, "On Security Analysis of Proof-of-Elapsed-Time (PoET)," Lecture Notes in Computer Science Stabilization, Safety, and Security of Distributed Systems, pp. 282-297, Oct. 2017.

[29] F. Ayaz, Z. Sheng, D. Tian and Y. L. Guan, "A Proof-of-Quality-Factor (PoQF) based Blockchain and Edge Computing for Vehicular Message Dissemination," IEEE Internet Things J., Dec. 2020.

[30] Islam, Shafkat, Shahriar Badsha, and Shamik Sengupta. "A light-weight blockchain architecture for v2v knowledge sharing at vehicular edges." In 2020 IEEE International Smart Cities Conference (ISC2), pp. 1-8. IEEE, 2020.

[31] Ayaz, Ferheen, Zhengguo Sheng, Daxin Tian, and Yong Liang Guan. "A blockchain based federated learning for message dissemination in vehicular networks." IEEE Transactions on Vehicular Technology 71, no. 2 (2021): 1927-1940.

[32] W.Y.B. Lim, N.C. Luong, D.T. Hoang, Y. Jiao, C. Liang, Q. Yang, D. Niyato and C. Miao, "Federated learning in mobile edge networks: A comprehensive survey," IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 2031-2063, Apr. 2020.

[33] S.R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," IEEE Trans. Comm, vol. 68, no. 8, pp. 4734-4746, Aug. 2020.

[34] Ayaz, F., Sheng, Z., Tian, D., Liang, G.Y. and Leung, V., 2020, June. A voting blockchain based message dissemination in vehicular ad-hoc networks (VANETs). In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

[35] Hu, W., Hu, Y., Yao, W. and Li, H., 2019. A blockchain-based Byzantine consensus algorithm for information authentication of the Internet of vehicles. IEEE Access, 7, pp.139703-139711.

[36] X. Wang, C. Wang, X. Li, V. C. M. Leung, and T. Taleb, "Federated Deep Reinforcement Learning for Internet of Things with Decentralized Cooperative Edge Caching," IEEE Internet of Things Journal, Apr. 2020.

[37] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing Proof-of- Stake Blockchain Protocols," Lecture Notes in Computer Science Data Privacy Management, Cryptocurrencies and Blockchain Technology, pp.297–315, Sep. 2017.