

# Secure Vehicular Communication through Blockchain-based fair Reward Mechanism



By

Fatima Asif

(Registration No: 00000327259)

MSIS-2020

Department of Computing

School of Electrical Engineering and Computer Science  
(SEECS)

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

(2024)

# Secure Vehicular Communication through Blockchain-based fair Reward Mechanism



By

**Fatima Asif**

(Registration No: 00000327259)

A thesis submitted to the National University of Sciences and Technology, Islamabad,

in partial fulfillment of the requirements for the degree of

Masters in

Information Security

Supervisor: **Dr. Huma Ghafoor**

School of Electrical Engineering and Computer Science (SEECS)


National University of Sciences and Technology (NUST)

Islamabad, Pakistan

(2024)


## THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "Secure Vehicular Communication through Blockchain-based fair Reward Mechanism" written by Fatima Asif, (Registration No 327259), of SEecs has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.


Signature: \_\_\_\_\_ 

Name of Advisor: \_\_\_\_\_ Dr. Huma Ghafoor

Date: \_\_\_\_\_ 26-Feb-2024

HoD/Associate Dean: \_\_\_\_\_ 

Date: \_\_\_\_\_ 19-03-24

Signature (Dean/Principal): \_\_\_\_\_    
 Dr. Muhammad Ajmal  
 Principal,  
 NUST School of Electrical  
 Engg & Computer Science  
 H-12, Islamabad

Date: \_\_\_\_\_ 19 MAR 2024

## Approval

It is certified that the contents and form of the thesis entitled "Secure Vehicular Communication through Blockchain-based fair Reward Mechanism" submitted by Fatima Asif have been found satisfactory for the requirement of the degree

Advisor : Dr. Huma Ghafoor

Signature: 


Date: 26-Feb-2024

Committee Member 1:Dr. Mohaira Ahmad

Signature: 

26-Feb-2024

Committee Member 2:Dr. Syed Ali Hassan

Signature: 

Date: 28-Feb-2024


Signature: \_\_\_\_\_

Date: \_\_\_\_\_

## Certificate of Originality

I hereby declare that this submission titled "Secure Vehicular Communication through Blockchain-based fair Reward Mechanism" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEECS or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEECS or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student Name: Fatima Asif

Student Signature:  \_\_\_\_\_

### Certificate for Plagiarism

It is certified that PhD/M.Phil/MS Thesis Titled "Secure Vehicular Communication through Blockchain-based fair Reward Mechanism" by Fatima Asif has been examined by us. We undertake the follows:

- a. Thesis has significant new work/knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
- b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.
- c. There is no fabrication of data or results which have been compiled/analyzed.
- d. There is no falsification by manipulating research materials, equipment or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
- e. The thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC plagiarism Policy and instructions issued from time to time.

#### Name & Signature of Supervisor

Dr. Huma Ghafoor

Signature : 

FORM TH-4

# National University of Sciences & Technology MASTER THESIS WORK

We hereby recommend that the dissertation prepared under our supervision by: (Student Name & Reg. #) Fatima Asif [327259]

Titled: Secure Vehicular Communication through Blockchain-based fair Reward Mechanism

be accepted in partial fulfillment of the requirements for the award of Master of Science (Information Security) degree.

### Examination Committee Members

1. Name: Mohaira Ahmad Signature: [Signature]  
15-Mar-2024 10:46 AM

2. Name: Syed Ali Hassan Signature: [Signature]  
15-Mar-2024 10:46 AM

Supervisor's name: Huma Ghafoor Signature: [Signature]  
15-Mar-2024 11:07 AM

[Signature]  
HoD/Associate Dean

19-03-24  
Date

### COUNTERSIGNED

19 MAR 2024  
Date

v

[Signature]  
Dr. Muhammad Ajmal  
Principal,  
NUST School of Electrical  
Engg & Computer Science  
1974, Islamabad  
Dean/Principal

## **DEDICATION**

Dedicated to my parents and siblings, who have consistently provided unwavering strength and support, guiding me through every decision. Their prayers have been instrumental in helping me achieve this milestone.



## **ACKNOWLEDGEMENTS**

I am deeply grateful to my Creator, Allah, for His constant guidance and inspiration throughout this journey. Every new idea and insight that enriched this work was a blessing from Him, and I am humbled by His invaluable assistance.

I extend my heartfelt thanks to my beloved parents, whose unwavering support has been a source of strength in every aspect of my life. Their encouragement has been a guiding light, and I am profoundly grateful for their love and sacrifices.

Special appreciation is due to my supervisor, Dr. Huma Ghafoor, whose guidance and patience have been indispensable throughout my thesis. Her mentorship has not only facilitated my research but has also deepened my understanding of the research process.

I am also thankful to Dr. Mohaira Ahmed and Dr. Syed Ali Hassan for their invaluable contributions as members of my thesis guidance and evaluation committee. Their insights and feedback have been instrumental in shaping this work.

Last but not least, I would like to express my gratitude to my friends Shawal Rehan, Hamda Ikram, Sania Saeed, Aleeha Noor, Khuram Ashraf, Syeda Wafa Zainab, and Usama Asif for their unwavering emotional support. Their encouragement has been a constant source of motivation, and I am thankful for their presence throughout this academic journey.

# Contents

<b>LIST OF FIGURES</b>	<b>X</b>
<b>ABSTRACT</b>	<b>XI</b>
<b>1 Introduction and Motivation</b>	<b>1</b>
1.1 Definitions . . . . .	1
1.1.1 Blockchain . . . . .	1
1.1.2 VANETs . . . . .	1
1.1.3 DSRC . . . . .	2
1.1.4 Spectrum Scarcity . . . . .	2
1.1.5 Cognitive Radio . . . . .	2
1.1.6 CR-VANETS . . . . .	2
1.1.7 Smart Contracts . . . . .	3
1.2 Introduction . . . . .	3
1.3 Motivation . . . . .	5
1.3.1 Problem Statement . . . . .	5
1.3.2 Contribution of Research . . . . .	6
1.3.3 Thesis Structure . . . . .	6
<b>2 Literature Review</b>	<b>7</b>
2.1 Introduction to VANETs . . . . .	7
2.1.1 Challenges in VANETs . . . . .	7
2.1.2 Consideration of Spectrum Scarcity . . . . .	8
2.1.3 Shortage of DSRC spectrum . . . . .	8
2.2 Improvements with Cognitive Technology . . . . .	8
2.2.1 Resource Allocation Scheme . . . . .	8
2.2.2 Addressing Malicious Nodes . . . . .	9

2.2.3	Cognitive Internet of Vehicles . . . . .	9
2.2.4	CR-VANETs as a Solution . . . . .	9
2.3	Implementation using Smart Contracts .....	10
2.4	Offline Blockchain Framework .....	10
2.5	Routing Scheme for Critical Information.....	10
2.6	Failure to address Spectrum Scarcity and Security .....	11
2.7	Need for Incentivization.....	11
2.8	Research Aim.....	11
<b>3</b>	<b>Research Methodology</b>	<b>12</b>
3.1	Proposed Concept .....	12
3.2	Experimentation Setup .....	14
3.2.1	Development Tools and Environment .....	14
3.2.2	Communication Channels and Parameters .....	14
3.2.3	Communication Range and Speed.....	15
3.2.4	Experimental System .....	15
<b>4</b>	<b>Results and Discussions</b>	<b>22</b>
4.1	Comparison with Reference Schemes.....	22
4.1.0.1	Execution Time (Read Message): .....	22
4.1.0.2	Execution Time (Send Message):.....	23
4.1.0.3	Delivery Time:.....	26
4.1.0.4	Overhead: .....	27
4.2	Discussion.....	29
<b>5</b>	<b>Conclusions and Recommendation</b>	<b>30</b>
5.1	Future Recommendation .....	31
	<b>References</b>	<b>33</b>

# List of Figures

3.1	Secure CR-VANETs using blockchain.....	14
3.2	Enabling the contract on ten Ethereum accounts. ....	17
3.3	Setting up an account. ....	18
3.4	Verification of all registered users.....	19
3.5	A message sent by the source vehicle.....	19
3.6	Representation of unverified messages sent by any sender. ....	20
3.7	The receiver has paid for the message. ....	20
3.8	The sender and miner have received their rewards. ....	21
3.9	The receiver finally reads the message.....	21
4.1	Performance comparison of execution time for read function in terms of number of transactions. ....	24
4.2	Performance comparison of execution time for send function in terms of number of transactions. ....	25
4.3	Performance comparison of delivery time in terms of number of miners. ....	27
4.4	Performance comparison of overhead in terms of number of miners.....	29

# Abstract

Security is an important consideration when delivering information-aware messages to vehicles that are far away from the current location of the information-sending vehicle. This information helps the receiver to save fuel and time by making wise decisions to avoid damaged or blocked roads. To ensure the safety and security of this type of information using blockchain technology, I propose a new cognitive vehicular communication scheme to transfer messages from source to destination. The primary user (PU) makes a public announcement about a free channel to all secondary users nearby and only gives it to authentic vehicles. The authenticity of vehicles is guaranteed by a roadside unit (RSU) that offers secure keys to any vehicle that joins this blockchain network. Those who participate in this network must pay a certain amount and receive rewards for their honesty that exceed the amount spent. To test the performance of various parameters, the proposed scheme utilizes the Ethereum smart contract and compares them to blockchain and non-blockchain methods. My results show a minimum delivery time of 0.16 seconds and a minimum overhead of 350 bytes in such a dynamic vehicle environment.

**Keywords:** Blockchain, cognitive radio (CR), primary user (PU), roadside unit (RSU), smart contract, vehicular ad hoc networks (VANETs)

# Chapter 1

## Introduction and Motivation

### 1.1 Definitions

This section will define some of the commonly used terms in this thesis that will be necessary for the reader to get a better understanding of this thesis research.

#### 1.1.1 Blockchain

Blockchain is like a digital record book that is shared across many computers in a network. Instead of being stored in one place, like a traditional ledger, it's duplicated and distributed to all the computers connected to the network. This means that everyone involved in the network has a copy of the same record book. Each time a new entry is added to the record book, it's automatically updated on every computer in the network. This makes it very difficult for anyone to alter or tamper with the information, providing a secure and transparent way to record transactions or data.

#### 1.1.2 VANETs

Vehicle Ad Hoc Network (VANET) is a type of network that helps vehicles communicate with each other and with roadside equipment. The goal of a VANET is to make driving safer and more efficient by allowing vehicles to share important information like traffic conditions or accidents. The network is made up of two main parts: the vehicles themselves and special equipment installed along the road called roadside units. Because vehicles are constantly moving quickly, the layout of the network is always changing, and sometimes the connections between vehicles and roadside units can be lost [1].

### **1.1.3 DSRC**

DSRC stands for Dedicated Short-Range Communication. It is a wireless communication technology specifically designed for communication between vehicles and roadside infrastructure, such as traffic lights and road signs, as well as among vehicles themselves. DSRC operates with a bandwidth of 75 MHz and enables high-speed, low-latency communication, making it well-suited for applications related to vehicle safety, traffic management, and cooperative driving.

### **1.1.4 Spectrum Scarcity**

Spectrum scarcity refers to the limited availability of radio frequency spectrum, which is the range of electromagnetic frequencies used for wireless communication. The radio frequency spectrum is a finite resource allocated by regulatory authorities for various purposes, including telecommunications, broadcasting, and wireless networking. As the demand for wireless communication services continues to grow rapidly, driven by the proliferation of mobile devices, IoT devices, and wireless technologies, the available spectrum becomes increasingly congested.

### **1.1.5 Cognitive Radio**

Cognitive radio is a wireless communication technology that enables radios to dynamically adjust their operating parameters based on the surrounding radio frequency environment and the user's communication needs. Unlike traditional radios, which operate on fixed frequencies and parameters, cognitive radios can sense their environment, analyze available spectrum, and adapt their transmission parameters (such as frequency, power, and modulation) to optimize communication performance and spectrum utilization.

### **1.1.6 CR-VANETS**

CR-VANET, or Cognitive Radio Vehicular Ad Hoc Network, is a type of network where vehicles communicate with each other and with roadside infrastructure using cognitive radio technology.

CR-VANET allows vehicles to intelligently access and utilize the available radio frequency spectrum while communicating on the road. This technology enables vehicles to dynamically adjust their communication parameters to avoid interference and optimize spectrum usage, thereby enhancing the reliability and efficiency of communication in vehicular environments. By integrating cognitive radio capabilities into VANETs, CR-VANETs aim to improve road safety, traffic management, and overall transportation efficiency [2].

### **1.1.7 Smart Contracts**

A smart contract is like a digital agreement where the rules are written in computer code. This code is stored on a network of computers called a blockchain, which is spread out and not controlled by any single entity. Smart contracts allow people to make deals and transactions with each other without needing a middleman, like a bank or a legal system, to oversee everything. It's like having a virtual handshake that automatically carries out the terms of the agreement once both parties agree to it, making transactions more secure and efficient [3].

## **1.2 Introduction**

As the world continues to progress, technology permeates every aspect of our daily lives, transforming everything from household appliances to entire living spaces with the advent of smart home systems. Similarly, entertainment has evolved from traditional video games to immersive virtual reality experiences, offering unprecedented levels of engagement and interaction. Moreover, advancements in automotive technology have transitioned vehicles from manual operation to the realm of self-driving cars, revolutionizing the way we perceive transportation. However, alongside these technological advancements, the challenges posed by an increasing global population necessitate innovative solutions to manage the complexities of modern life. The rise in population has led to a surge in car ownership as individuals seek to efficiently meet their family's transportation needs. Furthermore, the prevalent work culture, characterized by long commutes and extensive time spent on roads, underscores the importance of improving the overall travel experience [4].

In response to these evolving societal needs, research efforts are underway to facilitate seamless communication between vehicles while navigating the roads. Recognizing the significance of efficient vehicular communication in enhancing safety, optimizing traffic flow, and minimizing travel times, researchers are exploring novel approaches to enable vehicles to interact intelligently with each other and with surrounding infrastructure. These endeavors aim to harness the potential of emerging technologies such as cognitive radio and blockchain to create robust communication networks within the vehicular environment. By fostering communication and collaboration among vehicles, these initiatives seek to pave the way for a future where transportation is not only efficient but also safer and more sustainable. Thus, as the world continues to embrace technological innovation, the quest for enhancing vehicular communication stands as a testament to humanity's relentless pursuit of progress and improvement in all areas of life. As the concept of self-driving cars has come to life, there are procedures underway to secure pedestrians with some communication between cars and pedestrians as well [5].



Vehicular ad hoc network (VANET) is a growing technology that allows vehicles to communicate with each other, forming vehicle-to-vehicle (V2V) communications and with roadside units (RSUs), resulting in vehicle-to-roadside (V2R) communications using dedicated short-range communication (DSRC) technology. Vehicles exchange messages with each other or with RSUs using onboard units (OBU). This exchange of messages should be secure to avoid any miscommunication in such a highly dynamic environment. Any vehicle forwarding information that is beneficial for other vehicles on the road requires its privacy not to be compromised.

Every vehicle requires secure and authentic communications to prevent privacy breaches, which can only be achieved by encrypting the communication. To ensure authentication, every participating node has a public and private key pair stored in a secure database. For a decade now, blockchain has been an emerging technology that offers a distributed database made up of blocks of data interconnected as a chain [6]. It is famous for its decentralized and tamper-proof qualities. A peer-to-peer network manages the blockchain, with each node having a distinct public key. The public key is used to broadcast all transactions, and the node records them to form a block [7].

Forming a block requires periodic messaging in vehicles, which is critical when using the DSRC band due to its spectrum scarcity issue. Cognitive radio (CR) technology has been employed in vehicles that form a cognitive radio vehicular ad hoc network (CR-VANET) [8], allowing them to locate idle channels and establish a link between any source and destination. In CR-VANETs, secondary vehicles periodically sense the channel and, when they find it free, utilize it for communication, keeping the primary user's (PU) activity safe.

The PU monitors its channel activity, so when it becomes idle, the PU helps secondary nodes by allowing them to use its free spectrum only if they are authentic. The authenticity is proven by an RSU, which serves as a database to deploy a smart contract and provides secure key pairs to all vehicles that successfully register with the RSU. In addition, after registering, PU takes some amount from the vehicles that use its free spectrum. This ensures that the channel is used safely and securely. Moreover, to make my blockchain network a fair and secure mechanism for conveying any message, I introduce rewards to all nodes who participate in conveying any message that is beneficial for other vehicles on the road. In this way, I ensure that all nodes participating in this network are authentic and gain benefits by becoming part of this network and performing their duties honestly. To consider delivering information-aware messages while ensuring security using blockchain technology, I introduce a novel method of cognitive vehicular communication.

## 1.3 Motivation

In an era marked by rapid technological advancement, vehicular communication networks represent a critical frontier for innovation and improvement. As the world witnesses a proliferation of smart technologies and an increasing reliance on vehicular transportation, there arises a pressing need to enhance the efficiency, safety, and reliability of communication systems within the vehicular domain. Traditional approaches to vehicular communication face significant challenges, including spectrum scarcity and security vulnerabilities, which impede their ability to meet the evolving demands of modern transportation systems. Recognizing these challenges as opportunities for innovation, this research endeavors to develop a novel method of cognitive vehicular communication that addresses these concerns comprehensively.

The motivation behind this research stems from the transformative potential of cognitive vehicular communication systems in revolutionizing transportation networks. By leveraging emerging technologies such as blockchain and cognitive radio, this research seeks to overcome the limitations of traditional approaches and unlock new possibilities for efficient, secure, and information-aware communication among vehicles and roadside units. Furthermore, the increasing emphasis on information dissemination and real-time communication in vehicular networks underscores the urgency of developing robust and reliable communication solutions [9].

Through this research, we aim to contribute to the advancement of cognitive vehicular communication by introducing a method that optimizes spectrum utilization, ensures communication security, and fosters honest participation within the network. By addressing these key challenges, we strive to pave the way for a future where vehicular communication systems facilitate seamless interaction, enhance transportation efficiency, and promote safer and more sustainable mobility solutions. Ultimately, the motivation behind this research lies in harnessing the power of technology to create smarter, more connected, and more efficient transportation networks for the benefit of society.

### 1.3.1 Problem Statement

In the realm of vehicular communication networks, the coexistence of spectrum scarcity and the imperative of ensuring communication security poses significant challenges. Traditional approaches to vehicular communication often struggle to address these dual concerns effectively. Moreover, the increasing reliance on vehicular networks for information dissemination and communication underscores the need for innovative solutions that can reconcile these challenges. Thus, the problem at hand revolves around

devising a method that not only optimizes spectrum utilization but also ensures robust security measures in vehicular communication networks. This method should facilitate seamless communication among vehicles and roadside units while safeguarding privacy and authenticity. Additionally, there is a need for a fair and secure reward mechanism to incentivize honest participation and information sharing within the network. Addressing these challenges is crucial to realizing the full potential of cognitive vehicular communication systems in enhancing transportation efficiency, safety, and reliability.

### **1.3.2 Contribution of Research**

The primary contributions of my research can be summarized as follows:

- The consideration of two major concerns in vehicular networks: spectrum scarcity and security. Integrating blockchain technology in cognitive vehicular communication through a new method of spectrum sharing for primary and secondary users is one of the major contributions of this article.
- Another contribution is to provide a fair and secure reward scheme for cognitive vehicular communication that aims to convey information quickly and honestly.

### **1.3.3 Thesis Structure**

The remaining parts of this article are arranged in the following manner. Chapter 2 provides a literature review, Chapter 3 describes the Research Methodology, Chapter 4 shows Results and Discussions, and Chapter 5 concludes with Future Recommendations.

# Chapter 2

## Literature Review

In this chapter, we will be reviewing the existing literature about the domain of secure vehicle communication using blockchain. The research for the literature review was gathered from credible sources which include IEEE, ACM Digital Library, Science Direct, and Research Gate. The research papers were selected based on their relevance to the searched queries containing keywords related to the said domain.

### 2.1 Introduction to VANETs

The development in vehicular communication is evidence of the advancement in technology. In the early 2000s, when the VANETs were introduced, it was considered a remarkable milestone as it completely transformed the vehicular communication setup.

#### 2.1.1 Challenges in VANETs

However, two issues are currently the most common in VANETs. One is spectrum scarcity. VANETs rely on wireless communication for vehicles to exchange information with each other and with roadside infrastructure. However, the radio frequency spectrum allocated for vehicular communication is limited. As the number of vehicles and their communication needs increase, the available spectrum becomes insufficient to accommodate all communication demands. This scarcity can lead to congestion, degraded communication quality, and increased latency in transmitting critical information.

Security is another major challenge in VANETs. Due to the open and dynamic nature of vehicular environments, VANETs are vulnerable to various security threats, such as malicious attacks, spoofing, and data tampering. Securing communication

among vehicles and ensuring the authenticity, integrity, and confidentiality of transmitted data are critical for maintaining trust and reliability in VANETs. Without robust security measures in place, VANETs are susceptible to cyber-attacks, which can compromise safety, privacy, and the overall effectiveness of vehicular communication.

### **2.1.2 Consideration of Spectrum Scarcity**

To secure data in vehicular communication [10], an RSU was considered as a fog node that provides decentralized data privacy using blockchain technology. Latency and overhead were used as performance metrics when evaluating the scheme. Despite this, the vehicular scheme was conventional and did not take into account spectrum issues.

### **2.1.3 Shortage of DSRC spectrum**

As more and more devices use wireless communication, there's a growing concern that there won't be enough space in the dedicated short-range communication (DSRC) spectrum for everyone to communicate without interfering with each other.

## **2.2 Improvements with Cognitive Technology**

To address this issue of spectrum scarcity, a new type of radio technology called Cognitive Radio was developed. Cognitive Radio uses smart techniques to figure out which radio channels are being used and which ones are available. By doing this, it helps devices use the available space more efficiently, reducing interference and improving communication for everyone. The research explores how Cognitive Radio can make communication better by improving things like speed, reliability, and the amount of data that can be sent. [11]

### **2.2.1 Resource Allocation Scheme**

Volosin *et al.* [12] introduced a resource allocation scheme aimed at addressing the unique communication needs of autonomous vehicles, particularly considering their driving routes. Their innovative approach utilized blockchain technology to facilitate resource allocation and route planning for autonomous vehicles. By leveraging blockchain-based tokens, they could allocate resources and define routes for specific nodes over predetermined timeframes, thereby optimizing communication and navigation for autonomous vehicles. Looking ahead, their future direction involves extending their approach to incorporate vehicle-to-vehicle communication, recognizing

the importance of seamless interaction among vehicles for enhanced communication and collaboration on the road. This expansion promises to further improve the efficiency and effectiveness of autonomous vehicle communication systems, advancing the capabilities of future transportation networks.

### **2.2.2 Addressing Malicious Nodes**

Another scheme TOPSIS [13] combines cognitive concepts with blockchain technology to tackle the problem of malicious nodes in vehicular networks. This scheme enables vehicles to track both legal and illegal activities happening within the network. Essentially, it helps identify and prevent any unauthorized or harmful actions by certain nodes. However, the researchers noted that certain important aspects, such as delivery time and the amount of resources used for sensing, are still under development and will be addressed in future work.

### **2.2.3 Cognitive Internet of Vehicles**

In another study, researchers introduced a new idea called the cognitive internet of vehicles (IoV) in [14]. This concept aims to enable autonomous vehicles to share cognitive data with each other using a system of agreement called consensus, which involves cognitive engines. To ensure the reliability of this data-sharing process, the researchers utilized blockchain technology, which includes a method to evaluate the trustworthiness of participants. However, the authors mentioned that they plan to work on creating a system to reward and encourage active participation in the future. This indicates that while the idea shows promise, there's still more work to be done to encourage cooperation among autonomous vehicles for better communication and collaboration on the road.

### **2.2.4 CR-VANETs as a Solution**

CR-VANET [8], or Cognitive Radio Vehicular Ad Hoc Network, presents a promising solution to the challenges of spectrum scarcity in Vehicle Ad Hoc Networks (VANETs). With traditional VANETs facing limitations due to the limited availability of dedicated spectrum for vehicular communication, CR-VANET leverages Cognitive Radio technology to intelligently manage spectrum utilization. By dynamically adjusting communication parameters based on spectrum availability, CR-VANET optimizes spectrum usage while minimizing interference. Also, different security-based methods have been proposed in the literature [15] to provide trust-based communication in VANETs. To detect malicious nodes, the scheme ensured security and established trustworthiness.

## 2.3 Implementation using Smart Contracts

Das *et al.* [16] implemented a smart contract scheme (digital contracts written in solidity language where the conditions to work in the blockchain environment are described). The scheme explains the implementation in the areas of vehicle identification, user authentication, and communication. Once a vehicle registers itself on the blockchain network using the contract, the vehicle is identified and the user receives unique public and private key pairs to communicate within the zone. The vehicle can also communicate with vehicles in other zones if they have cellular networks. The thing that is not addressed in this is how it will deal with the increasing number of vehicles registered on the network.

## 2.4 Offline Blockchain Framework

Similarly, in an offline blockchain framework [17] researchers introduced an offline blockchain framework designed to store information from participating nodes for future reference. This framework enables nodes within a network to record and store data securely, ensuring that it's available for later analysis or use. Unlike traditional online blockchain systems that operate in real-time, this offline framework doesn't consider immediate delays in the data processing. Additionally, it doesn't account for the amount of resources consumed during data storage and retrieval, focusing solely on securely storing information for future purposes. This approach offers a method for preserving data integrity and accessibility within a network, paving the way for potential applications in various domains where data retention and analysis are crucial.

## 2.5 Routing Scheme for Critical Information

BBSF (blockchain-based secure weather forecasting) [18] is a routing scheme in which researchers proposed a method to enhance data security in vehicular communication using blockchain technology. They suggested using Roadside Units (RSUs) as fog nodes, which act as intermediaries between vehicles and the central network. These fog nodes would employ blockchain to ensure decentralized data privacy, making it difficult for unauthorized parties to access or tamper with the information exchanged between vehicles and the network. The researchers evaluated the effectiveness of this approach using metrics such as latency (delay) and overhead (additional processing required). However, it's noted that while this method addresses data security concerns, it doesn't account for issues related to the availability of radio frequency spectrum, which is essential for efficient communication among vehicles.

## **2.6 Failure to address Spectrum Scarcity and Security**

All the schemes discussed above have failed to address the problems of spectrum scarcity and communication security simultaneously by mutually sharing spectrum between primary and secondary users and assessing delivery time and overhead consumption as performance metrics. They mostly looked at things like how fast messages are sent or how much extra work is needed, instead of looking at the overall impact on both radio space and communication safety. So, we need more research to come up with better solutions that deal with both these problems together. We also need to look at how well these solutions work in the real world by using the right measures to see how much they help with radio space and communication safety at the same time.

## **2.7 Need for Incentivization**

As vehicle communication is necessary to inform vehicles on the road about any upcoming problem timely, we need to make sure that drivers take part in the idea of making the road safety experience even better. Why would someone want to invest their time in informing someone of a potential roadblock ahead? Why would someone spend money for the betterment of other people on the roads if they don't know whether other people will do the same for them or not? To make them do this, we need to reward them to take part in the betterment of our society. Multiple schemes [19] have experimented with giving incentives to people in return for a favor.

## **2.8 Research Aim**

This research aims to explore the efficiency of implementing blockchain technology to enhance security in cognitive vehicular communication and to evaluate how a fair reward mechanism can influence vehicles to participate in road safety and help reduce road incidents.



# Chapter 3

## Research Methodology

The purpose of this chapter is two-fold. Firstly, we will be discussing the proposed concept. Secondly, we will be going over the experimentation setup required to execute the process.

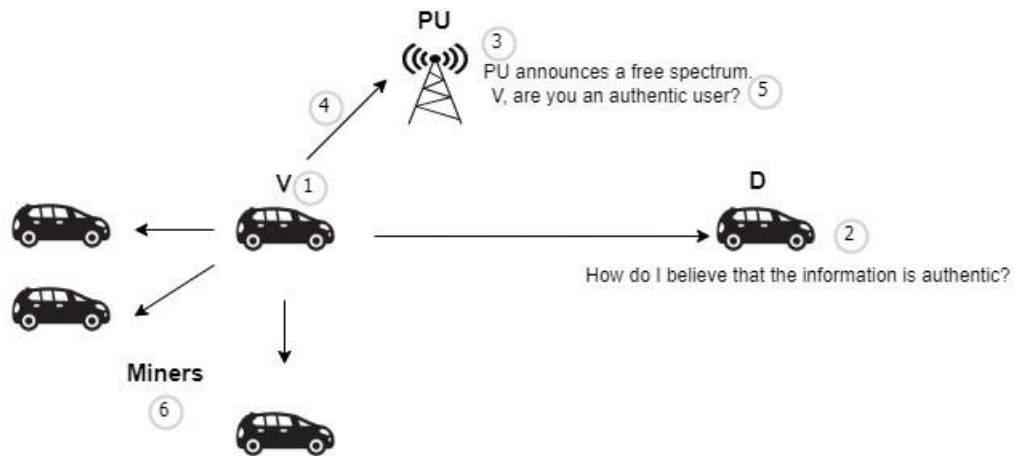
### 3.1 Proposed Concept

To guarantee the authenticity of all vehicles on the road, we propose a cognitive vehicular communication by deploying a smart contract on the blockchain network. Two RSUs are used in this scheme: one that deploys a smart contract and is responsible for monitoring communication, while the second acts as the PU. PU allows secondary users (vehicles) to use its channel by paying a minimal fee so that the channel remains authentic and the vehicles trying to communicate on this channel are all legitimate. We introduce a novel way of implementing cognitive technology, where PU is aware of secondary users who are using its channel and only allows them to access it if the channel is free and if they pay a minimal fee. When the channel was sensed free, any secondary user could access it in a conventional cognitive scheme, which increased the likelihood of fake nodes participating in the communication. In our scheme, the payment ensures that only those nodes participate in the network who are legitimate and willing to provide benefits to other nodes in the network. However, those who participate in this blockchain network will receive a reward that is higher than the amount they spent conveying messages. The verification process starts with the registration of each node. Each node registers itself when RSU deploys a smart contract. Each vehicle receives a secure ID in the same way as done in [19] which is an encrypted version of the vehicle ID to make communication secure. In this manner, only those nodes that are authentic can communicate using this secure ID. In the next section, we will provide a detailed explanation of the connection

between vehicles and RSU, how IDs are used, and how payment is made.

PU executes its tasks regularly. When there is no activity ongoing, which means it has a free spectrum, it announces this to all the nodes in its range. As can be seen by Fig. 3.1, the sender  $V$  witnessed an incident at its current location and wants to share that information with a destination  $D$  that is not within the sender's communication range. Because both  $V$  and  $D$  are authentic users who have validated their authenticity by registering with RSU, they can easily exchange messages using relays. It should be noted that all vehicles that are part of this blockchain network can access the RSU and register from their respective locations. Deploying smart contracts and approving the authenticity of vehicles is the only function of RSU in our scheme. Now, because  $V$  has some information to share, it requests a spectrum from PU by paying a minimal fee. A control channel is used to make this request.  $V$  uses this spectrum to reach  $D$  by making an ad hoc network. The message is carried and forwarded to  $D$  by a relay within  $V$ 's communication range who is willing to participate in the network. We consider only two-hop communications in this scheme. We will extend it in the near future by considering both city and highway scenarios. In this network, it is crucial to have both relays and miners. Any node that is within the communication range of a sender can be considered a relay. Miners are only authentic nodes that pay a fee to deliver messages to the destination and are all witnesses to incidents and validate the messages generated by the source. To join a blockchain network, the miner pays a fee and receives a reward from the destination upon honesty in fulfilling its task. Miners are volunteers but relays are not.

Miners can be a single node or more than one depending on who wants to get a reward by paying a minimal amount from their account. Since the information (for example, roadblock) will be beneficial to  $D$ , receiving that information will allow  $D$  to reroute its travel, which will save fuel and time. The rewards will be willingly given to those who aid  $D$  in providing this information. So the complete path for communication is from source to miner to destination. To put it briefly, PU has more coins in its wallet due to the free channel it offers to  $V$ .  $V$  makes a message for  $D$  after confirming its authenticity from the RSU. A miner validates this message by paying some coins and forwarding it to  $D$ . Miner is a node that has both sender and destination in its communication range. After receiving the message, the destination reads it, pays both the sender and miner as a token of appreciation and finally changes its route.



1. V has some information to share. But, how to communicate with D?  
(Requires common free spectrum)
2. Also, how D believes that the information is authentic.
3. PU announces a free spectrum.
4. Sender V asks for free spectrum.
5. Are you an authentic user?
6. Needs to validate its authenticity by aggregating the message from miners.

Figure 3.1: Secure CR-VANETs using blockchain.

## 3.2 Experimentation Setup

### 3.2.1 Development Tools and Environment

In developing my proposed vehicular communication scheme, I employed Solidity as the contract compiler, with Remix-Ethereum serving as the integrated development environment (IDE). This setup enabled us to effectively utilize Solidity for contract development, a crucial aspect of integrating blockchain technology into our system. For testing the blockchain aspect, we used Ganache, a popular choice for simulating Ethereum blockchain environments.

### 3.2.2 Communication Channels and Parameters

Our choice of 1 MHz from the Dedicated Short-Range Communications (DSRC) spectrum as the control channel, and 2 MHz as a service channel, was strategic. Within this 2 MHz bandwidth, we dedicated one portion exclusively to Primary User (PU) activities to ensure uninterrupted and secure communications, while the other portion was allocated to secondary users. This allocation was governed by an exponen-

tial on/off activity pattern with a rate parameter of 0.5 to optimize the spectrum usage.

### 3.2.3 Communication Range and Speed

The communication range set for the Roadside Unit (RSU) was 500 meters, and a vehicular range of 200 meters was employed. All vehicles in our simulation moved at a constant speed of 10 meters per second.

### 3.2.4 Experimental System

To evaluate the system's performance, we created a network comprising ten accounts, representing eight vehicles, one RSU, and one PU. Each account started with an initial allocation of 100 ethers, except the RSU account, which showed a lower balance as depicted in Figure 3.2. This was due to the deployment of the contract by the RSU, which required a minimal amount to be deducted as a gas fee. Interestingly, the PU account had a higher balance (110 ethers) than the initial allocation because it provided a free channel.

Our setup process included creating various accounts using the 'createAccount' functionality in Remix-Ethereum. For example, by accessing the third blockchain account, we established the sender account, as shown in Figure 3.3. Similarly, we created the receiver account and other participant accounts. It's important to note that every time a vehicle registered itself on the blockchain, a small registration fee was deducted from its wallet. This process, along with the 'getAllUsers' feature, allowed us to verify all registered users on our blockchain network, ensuring that every participant was authenticated and accounted for, as seen in Figure 3.4.

The scheme we developed facilitated secure and efficient communication between vehicles. For instance, in our example scenario, a source vehicle  $V$  wanting to send a message to a destination node  $D$  would first obtain the destination's address from the 'AllUsers' functionality as in 3.5. However, direct communication was not possible, necessitating the use of relays or miners in our scheme. For the message to reach  $D$  successfully, it had to be verified by at least one miner to authenticate the information and prevent any potential misinformation. This process is illustrated in Figure 3.6, where the message remains in the 'getAllUnverifiedMessages' feature until a miner close to the incident verifies it. If no miner verifies the message, it remains unverified and inaccessible to  $D$ . The verification process by miners plays a crucial role in maintaining the integrity of the information being transmitted.

Once a message is verified,  $D$  is required to pay both the sender and the participating miner before it can access the message. This payment serves as a reward for the sender for initiating the communication and for the miner for their role in the verification process, as depicted in Figure 3.7. After the payment is made, both the sender and the miner receive a higher amount than what was originally deducted from their wallets, incentivizing their participation in the network. This mechanism not only ensures the authenticity and reliability of the information but also encourages active participation in the network. The final step, as shown in Figure 3.8, is the increase in wallet balances of both  $V$  and the miner, followed by  $D$  being able to read the message (Figure 3.9).

Overall, our scheme offers a robust framework for secure and efficient vehicular communication, ensuring that every transaction and message transmission is authenticated and reliable, thereby enhancing the overall safety and efficiency of the vehicular network.

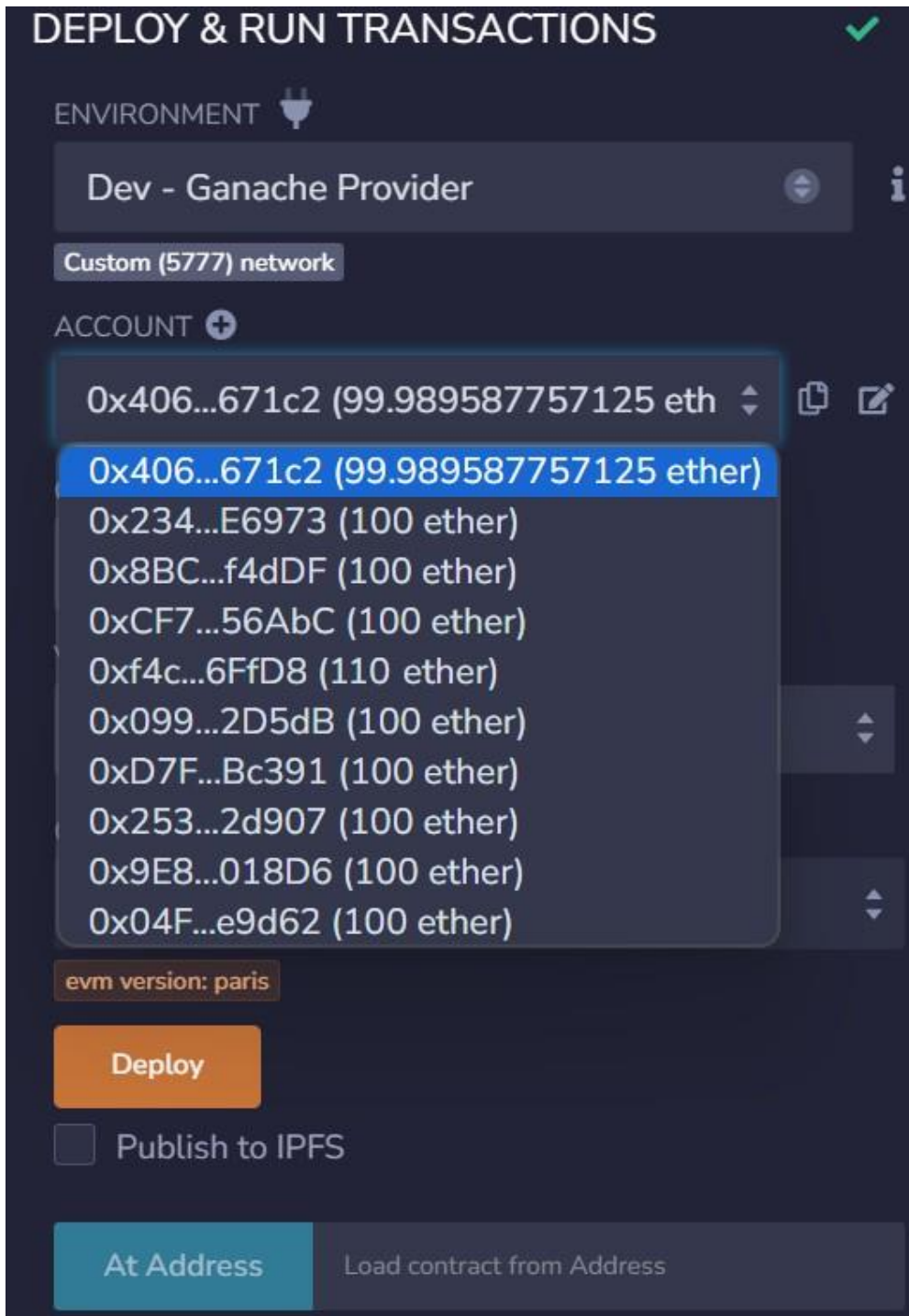


Figure 3.2: Enabling the contract on ten Ethereum accounts.

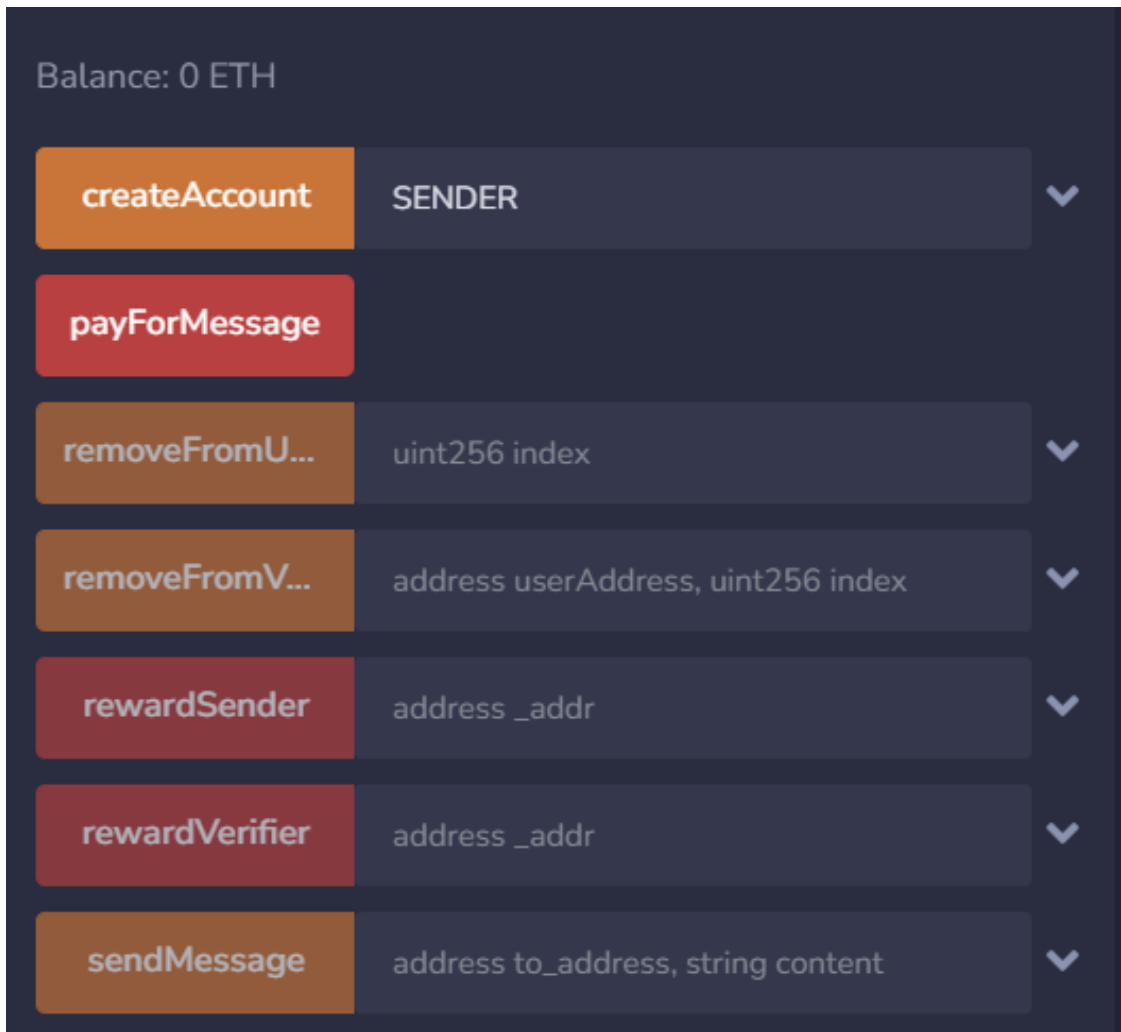


Figure 3.3: Setting up an account.

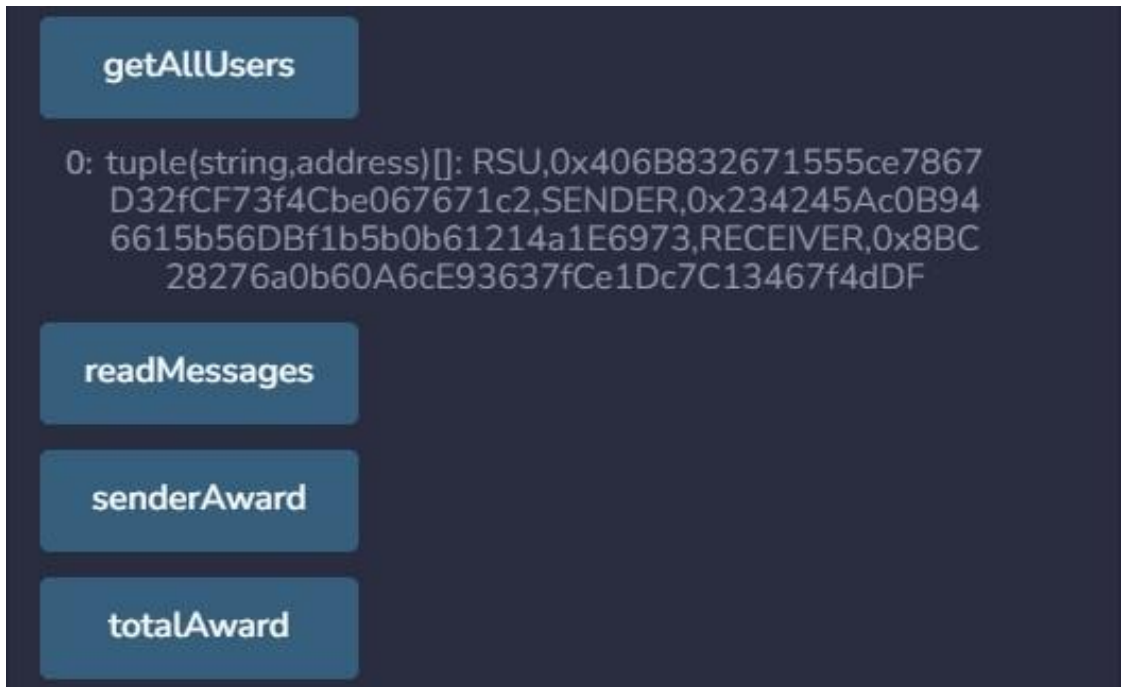


Figure 3.4: Verification of all registered users.

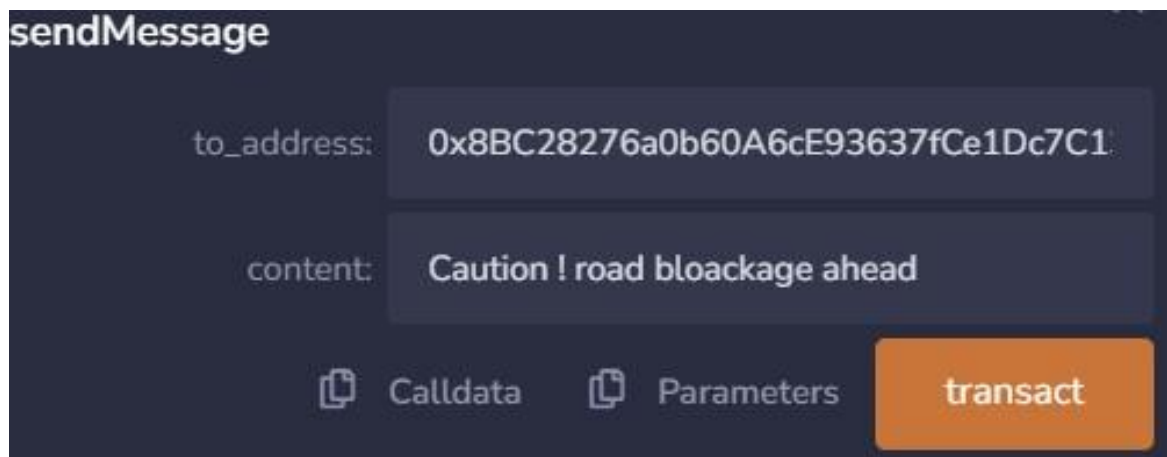


Figure 3.5: A message sent by the source vehicle.



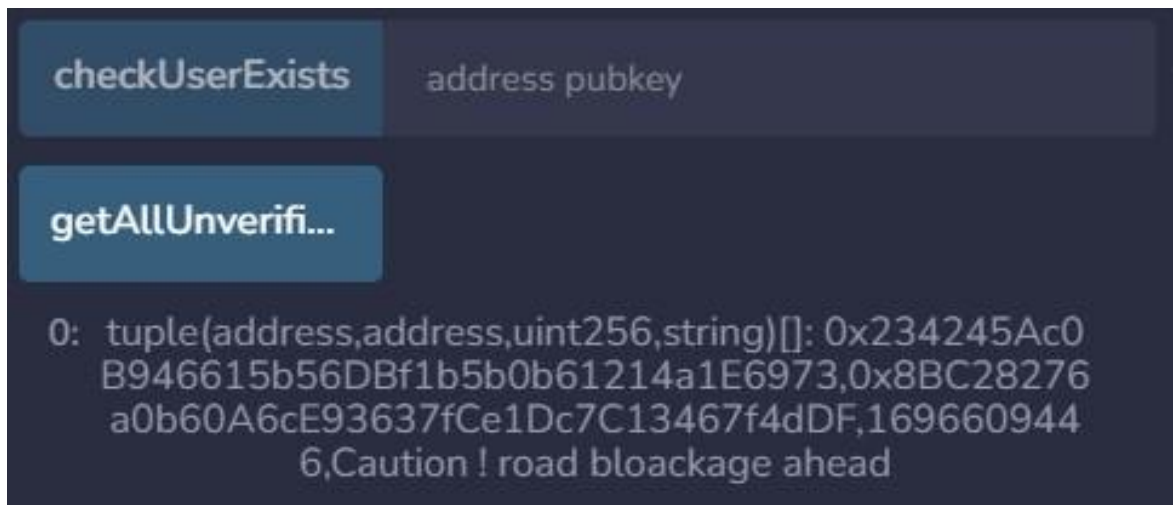


Figure 3.6: Representation of unverified messages sent by any sender.

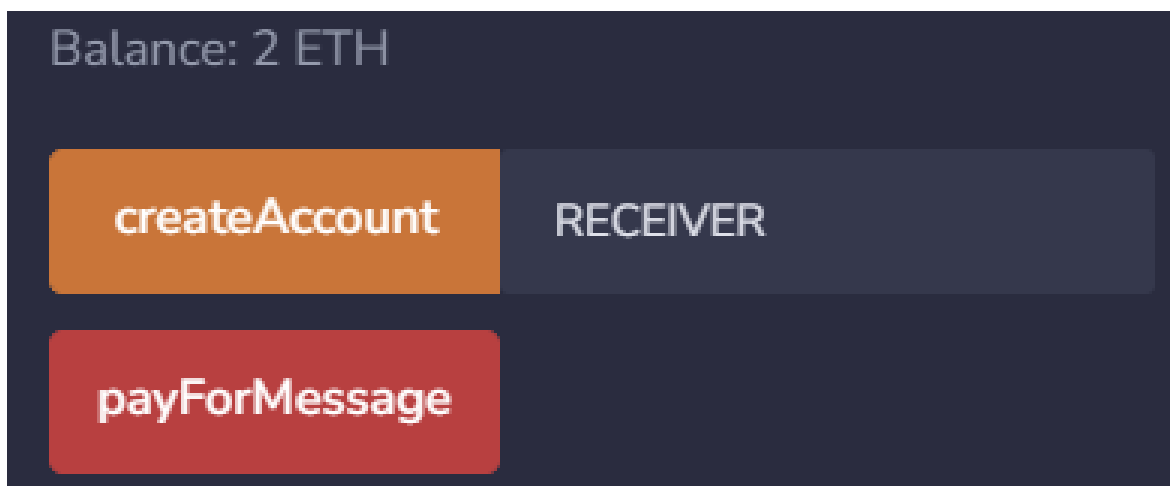


Figure 3.7: The receiver has paid for the message.

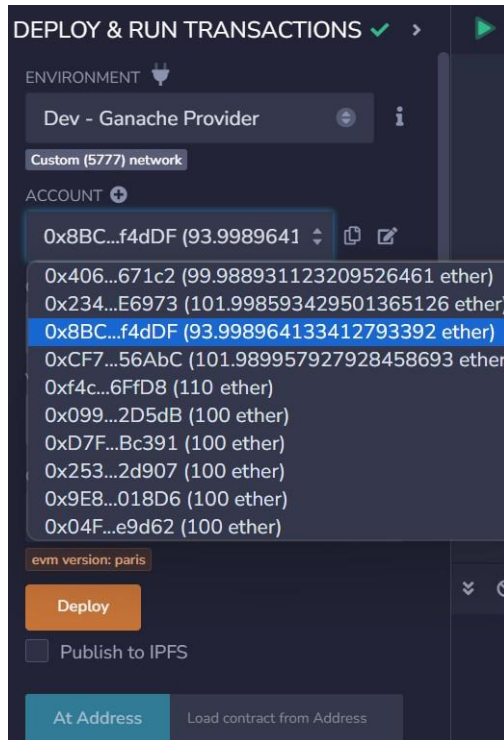


Figure 3.8: The sender and miner have received their rewards.

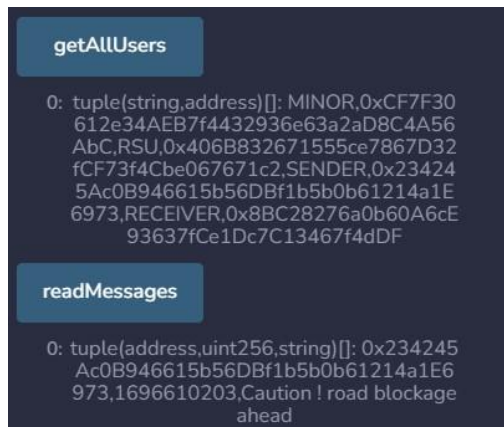


Figure 3.9: The receiver finally reads the message.

# Chapter 4

## Results and Discussions

In this section, we will discuss the results and also compare them with other reference schemes to see how well is our scheme performing.

### 4.1 Comparison with Reference Schemes

To evaluate the performance of the proposed scheme, I have taken into consideration different references. This means that instead of relying on a single metric or standard for evaluation, I compared multiple aspects of the system's performance against different benchmarks or reference schemes. This approach allows for a more comprehensive assessment of how the proposed system performs under various conditions and scenarios. It also helps in identifying specific areas where the integration of cognitive technology and blockchain networks offers the most significant improvements, as well as any potential limitations or challenges that may need to be addressed in future research.

#### 4.1.0.1 Execution Time (Read Message):

The 'Read Message Function' performance, as illustrated in Figure 4.1 of the thesis, is a critical aspect demonstrating the efficiency of the proposed system. This function's execution time is notably lower than that of the reference model across various transaction counts, highlighting the system's superior performance. This trend is particularly significant because it demonstrates the system's robustness and capability to handle high volumes of transactions without a significant increase in execution time. Such efficiency is crucial in vehicular systems where the speed of communication can directly impact the effectiveness of the network in real-world scenarios. The ability to maintain low execution times despite increasing transaction loads indicates

a well-optimized system that can handle the dynamic and often demanding environment of vehicular networks.

This robustness and swiftness in processing incoming messages are essential for real-time responsiveness in vehicular systems. Real-time responsiveness is vital for a range of applications in vehicular networks, from basic communication between vehicles to more complex scenarios like emergency response, traffic management, and autonomous driving. In these scenarios, delays in message delivery can have significant consequences, including reduced efficiency and even safety risks. Therefore, the system's ability to maintain low execution times even under high transaction loads is not just a technical achievement but also a practical necessity. It ensures that the network can reliably support the diverse and time-sensitive needs of modern vehicular systems, making it a suitable solution for the fast-paced and interconnected environment of smart cities.

#### **4.1.0.2 Execution Time (Send Message):**

The 'Send Message Function', as depicted in Figure 4.2 of the study, further solidifies the proposed system's high-performance capabilities. This function exhibits a pattern of enhanced performance, consistently outperforming the reference model across a range of transaction tests. The significant reduction in execution times during these tests is indicative of the system's efficient handling of message sending processes. Such efficiency is crucial in vehicular communication networks where the timely sending of messages is essential for the smooth functioning of various applications, from traffic management to emergency response systems. The ability of the system to maintain lower execution times, even as transaction volumes increase, demonstrates its robustness and reliability. This is particularly important in scenarios where rapid communication can be the difference in critical situations, such as collision avoidance or real-time traffic updates.

This improved performance in outbound communications underscores the system's capacity to maintain a steady and efficient flow of information throughout the network. Efficient outbound communication is a critical component in vehicular networks, ensuring that messages are not only received but also transmitted quickly and reliably. This capability is vital for the integrity and effectiveness of the entire communication system within smart city infrastructures. It ensures that vehicles can communicate with each other and with infrastructure components effectively, supporting a range of functionalities from autonomous driving to smart traffic control. The system's ability to handle high volumes of outbound communications with lower execution times also suggests its potential scalability, making it a viable solution for the growing demands of modern vehicular networks and smart city applications.

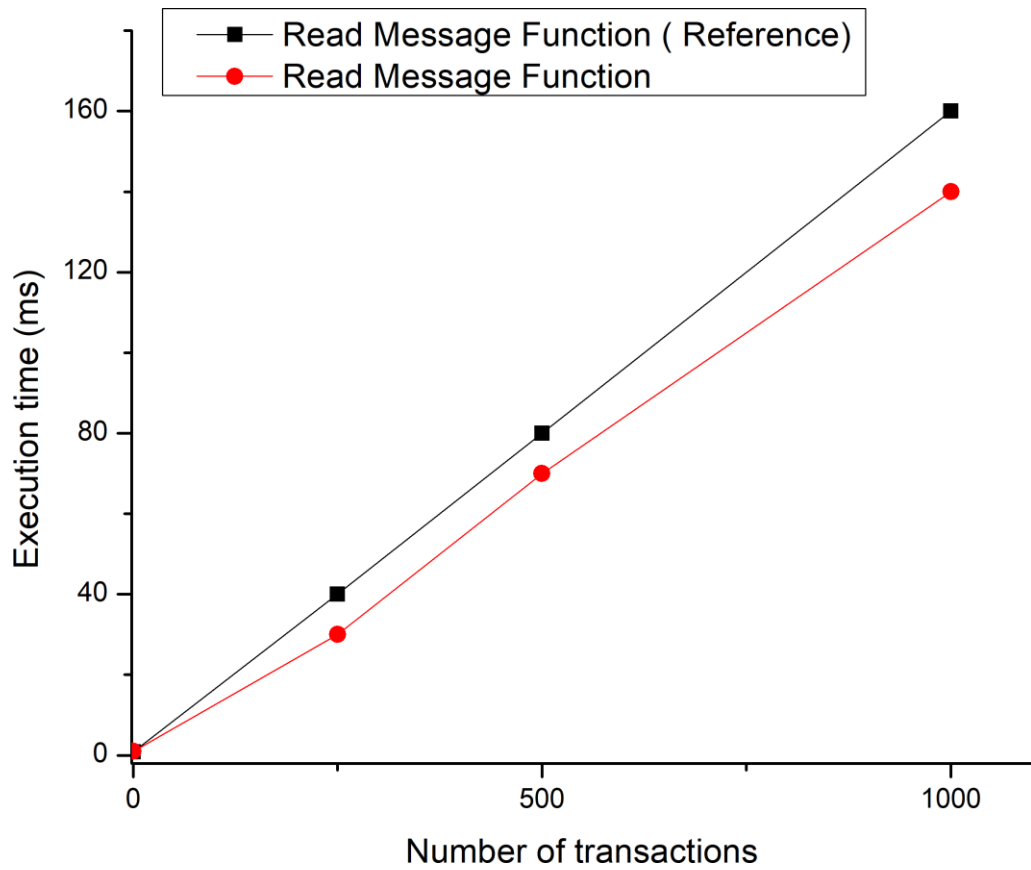


Figure 4.1: Performance comparison of execution time for read function in terms of number of transactions.

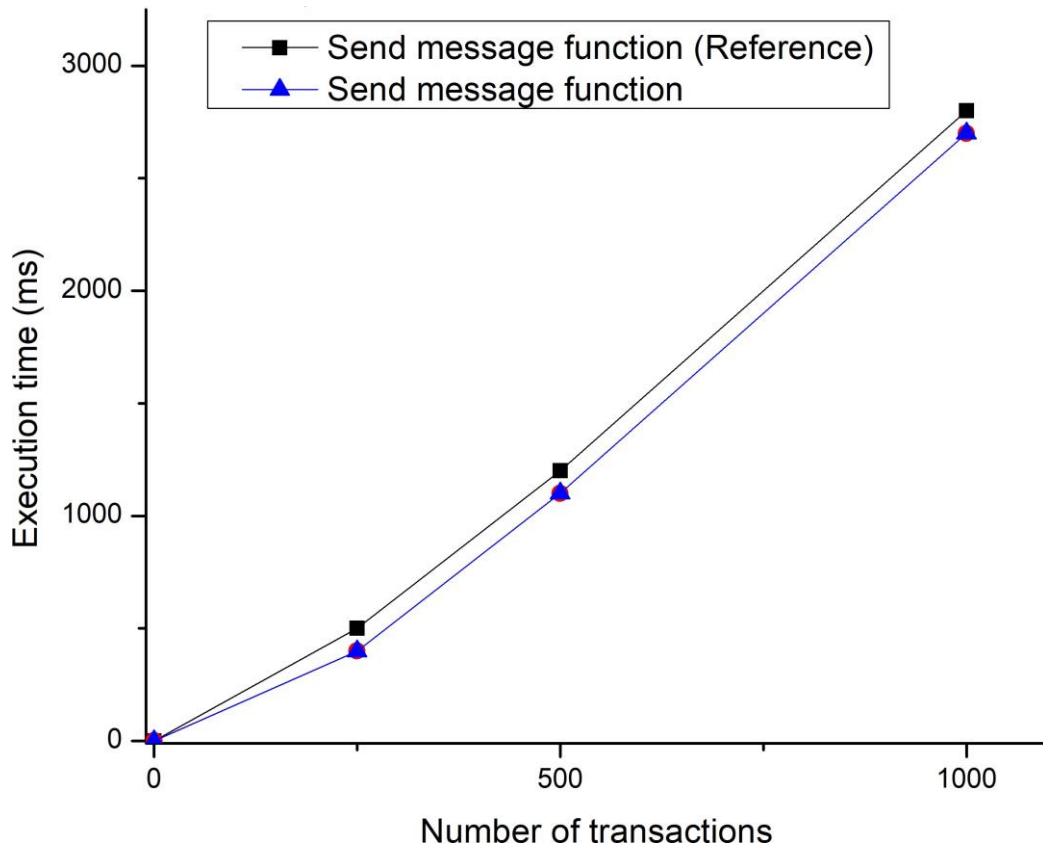


Figure 4.2: Performance comparison of execution time for send function in terms of number of transactions.

In the study, a comprehensive comparison was made between the proposed scheme’s reading and sending functions and a reference scheme [20]. This comparison revealed a superior performance of the proposed scheme, particularly evident as the number of transactions within the network increased. Typically, as transaction volumes rise, execution times tend to increase due to the added processing load. However, the proposed scheme demonstrated a notable deviation from this trend. This divergence is primarily attributed to the implementation of Roadside Units (RSUs) as central entities responsible for registering all nodes before communication commences. This preemptive registration process streamlines communication, allowing the system to process messages more swiftly than the reference scheme, even under high transaction loads. Such efficiency is crucial in vehicular networks, where real-time response capabilities are not just beneficial but often necessary for safety and efficient operation.

The cognitive aspect of the proposed scheme further enhances its performance and

safety features. In this system, nodes begin communication only after the Primary User (PU) has provided them with a channel. This approach ensures that the PU's activity remains secure and unimpeded, adding an extra layer of safety and efficiency to the network's operations. By securing and streamlining the channel allocation process, the scheme not only saves time but also reduces the likelihood of communication errors or delays. This aspect of the system underscores its capacity to handle outbound communications effectively, which is a critical factor in maintaining a steady and reliable flow of information across the network. Efficient outbound communication is essential in vehicular networks, supporting everything from routine traffic management to critical responses in emergencies. The system's ability to manage these communications swiftly and securely positions it as a highly effective solution for the evolving demands of smart city infrastructures and modern vehicular networks.

#### **4.1.0.3 Delivery Time:**

In our study, we meticulously compared our proposed vehicular communication scheme with two established reference models to evaluate its performance in terms of message delivery times and network overhead. The first model, known as the reference blockchain scheme, is primarily focused on securing the safety of travelers [21]. It employs the robustness of blockchain technology, particularly through the use of smart contracts, to ensure a secure and reliable routing system for both customers and drivers. This approach leverages the decentralized and immutable nature of blockchain to enhance the safety aspect of vehicular travel. The second model we compared against, the reference cognitive scheme, integrates cognitive radio technology in vehicular networks [8]. This model is designed to enable efficient packet delivery from a source node to a destination node, but it operates on the condition that a communication channel is available between these two nodes.

Our findings, which we detailed in Figure 4.3 of our thesis, shed light on the impact of the number of miners in the network on the delivery time of messages. We discovered that an increase in the number of miners within the network correlates with a decrease in the time it takes for a message to be delivered to its intended destination. This significant improvement in delivery time can be attributed to two key factors. Firstly, a greater number of miners in the network enhances overall connectivity. In a vehicular network that is inherently dynamic and constantly changing this enhanced connectivity is vital for the swift and efficient delivery of messages. Secondly, the presence of more miners in the network streamlines the process of validating the authenticity of messages, leading to a quicker overall delivery time. However, it's crucial to understand the operational differences between these schemes. The reference blockchain scheme, while focusing on route safety for

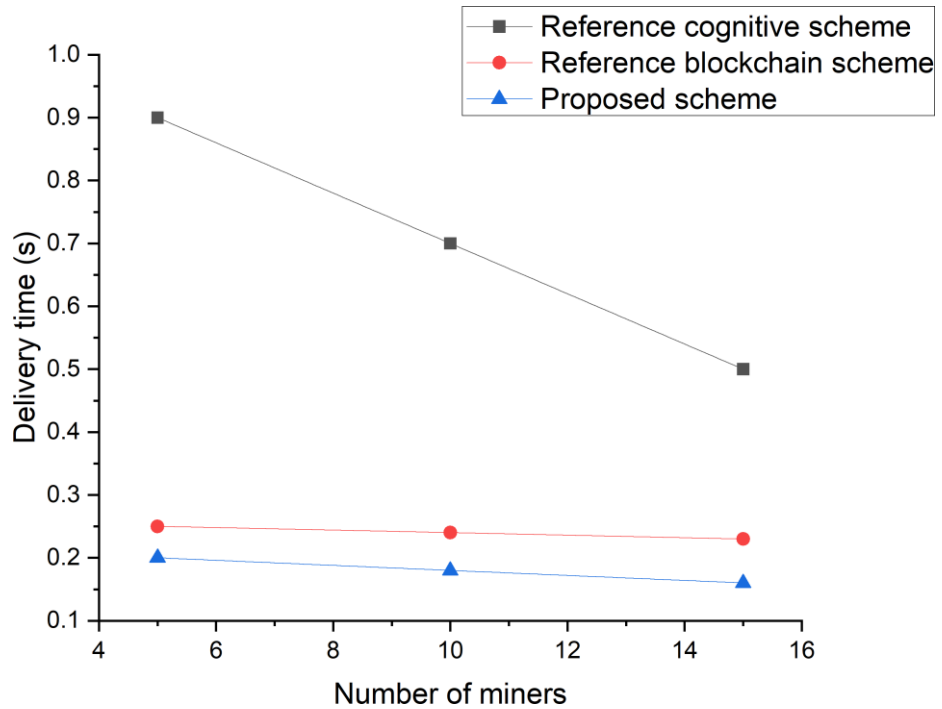


Figure 4.3: Performance comparison of delivery time in terms of number of miners.

users of a navigation app, tends to exhibit increased message delivery times with the addition of miners. This is contrasted with the reference cognitive scheme, where miners act as simple relays. Their role involves sensing the channel at every link, which, while beneficial for certain aspects of network performance, leads to longer message delivery times. Through this comparative analysis, the advantages of our proposed scheme become evident, particularly in its ability to balance the dual needs of safety and efficiency. Our scheme’s approach in optimizing message delivery times, while ensuring secure communication channels, highlights its potential as an effective solution for the evolving demands of smart vehicular networks.

#### 4.1.0.4 Overhead:

In our study, this pattern of efficient performance is further illustrated in Figure 4.4, where we analyze the overhead associated with our proposed scheme compared to other models. Overhead in a vehicular network is a critical factor, as it directly impacts the network’s efficiency and the speed at which data can be transmitted and



processed. To evaluate this, we considered a reference blockchain scheme [22], which is designed to provide a secure route by aggregating information from all vehicles and subsequently relaying it to a fog node. This approach, while secure, tends to increase network overhead, particularly as the number of nodes and the consequent exchange of messages rise. As more nodes communicate within the network, the volume of data being processed and transmitted grows, leading to higher overhead and potentially slower overall network performance. However, our proposed scheme demonstrates a notable advantage in this regard. By designating the Roadside Unit (RSU) to handle node authentication and the Primary User (PU) to manage channel provisioning, our system streamlines these processes, thereby reducing the burden on the network. Once these entities have fulfilled their roles, the nodes in the network can commence communication quickly and efficiently. This not only reduces the time taken for message delivery but also minimizes the overhead involved in managing these communications.

Our scheme's approach highlights a remarkable balance between the inherently resource-intensive nature of blockchain technology and the stringent efficiency requirements of vehicular networks. Blockchain, known for its security and transparency, can often lead to increased computational and communication demands. However, by smartly integrating this technology with the cognitive radio aspects of vehicular communication, our scheme manages to mitigate these demands. This is achieved without compromising the security and integrity of the communication channels, which is paramount in any vehicular network. Furthermore, the system's reward mechanism incentivizes rapid data delivery, ensuring that nodes have a tangible benefit to participate actively in the network. This not only enhances the efficiency of the network but also encourages a cooperative and dynamic communication environment.

Overall, our proposed scheme stands out as an effective solution for smart vehicular networks, adeptly balancing security, efficiency, and practicality to meet the evolving demands of modern urban transportation systems.

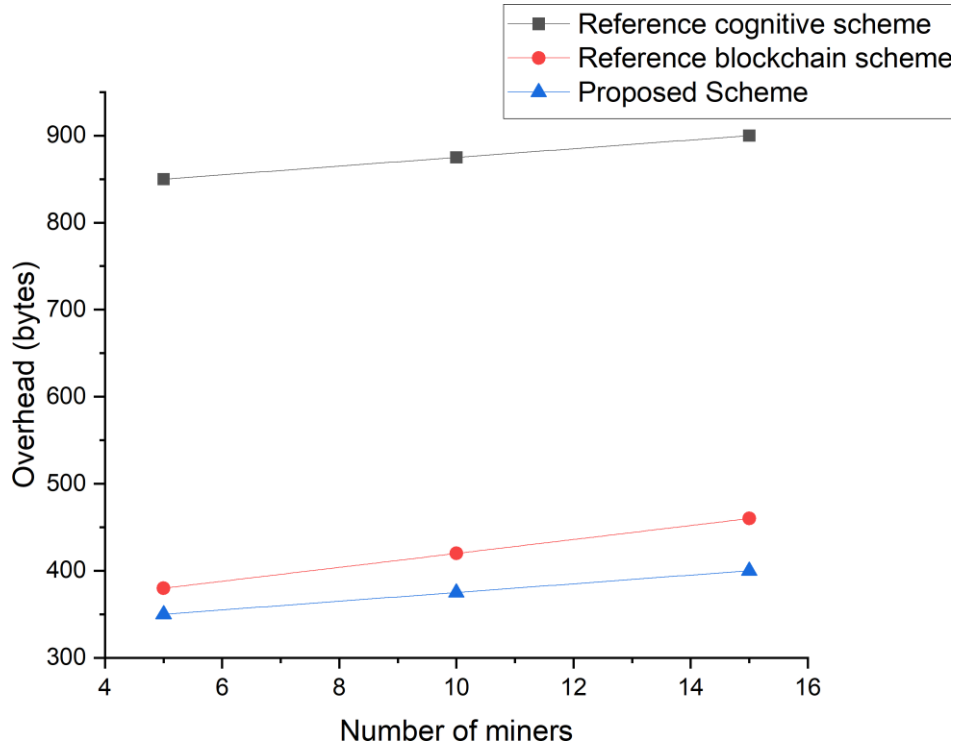


Figure 4.4: Performance comparison of overhead in terms of number of miners.

## 4.2 Discussion

The collective results from the performance metrics—delivery time, communication overhead, and execution time for message functions—paint a comprehensive picture of the system’s capabilities. Our proposed scheme notifies an impressive balance between the inherently resource-intensive nature of blockchain technology and the stringent efficiency requirements of vehicular communication systems. The consistent out-performance in message function execution times is particularly noteworthy, suggesting that our system can maintain high throughput and low latency, which are crucial for the implementation of blockchain in vehicular environments where performance and safety are closely intertwined. Moreover, the results provide clear evidence of the advantages of our optimized blockchain scheme over traditional models, especially in scenarios where rapid message dissemination and verification are critical. This evidence solidifies our system’s potential for deployment in real-world vehicular communication scenarios, where the benefits of blockchain can be harnessed without compromising on operational efficacy

# Chapter 5

## Conclusions and Recommendation

The research proposes a novel cognitive scheme for securing vehicular communications using blockchain technology. This is a type of cognitive communication in which PU announces its free channel to any authentic secondary user upon payment. All vehicles confirm their authenticity by registering with the RSU. A PU provides a channel to the source node only when a source node has some information to forward and it pays a certain amount for using the channel. The message which the source intends to deliver to the destination is verified only if at least one miner validates it. Miners are vehicles that volunteer to assist the destination in conveying the source message. Miners validate this message by paying a small amount from their wallets to receive a large reward from the destination. This message enables the destination to save fuel and time by rerouting its travel. The destination pays both the sender and the miner when it receives this beneficial message. Our findings indicate that execution time, delivery time, and overhead are less compared to other reference schemes.

## 5.1 Future Recommendation

Based on the findings and conclusions drawn in the thesis the following recommendations can be made for future research and practical applications:

1. **Scalability and Network Efficiency:** As vehicular networks continue to grow, especially in smart cities, it is crucial to focus on scalability. Future research should explore how this cognitive communication scheme can efficiently scale up to accommodate an increasing number of vehicles without compromising on execution time, delivery time, and network overhead.
2. **Enhanced Security Protocols:** While the current scheme shows promise in securing vehicular communications, continuous advancements in cybersecurity threats necessitate ongoing enhancements in security protocols. This includes the development of more robust cryptographic methods and secure communication channels.
3. **Economic and Incentive Models:** The current reward mechanism plays a significant role in ensuring the participation of vehicles in the network. Further research should delve into optimizing this economic model to ensure sustained engagement from users. This could involve dynamic pricing models that adapt to network conditions and user behaviors.
4. **Integration with Other Smart City Infrastructure:** The proposed scheme should be explored in the context of broader smart city infrastructure. This includes integration with other IoT devices, traffic management systems, and emergency response systems, creating a more cohesive and responsive urban environment.
5. **User Privacy and Data Protection:** Given the importance of user privacy in vehicular networks, future iterations of this scheme should place a greater emphasis on privacy-preserving techniques. This could involve the implementation of anonymization protocols or advanced data encryption methods to protect user identities and sensitive information.
6. **Real-world Testing and Deployment:** Practical implementation and testing in real-world scenarios are essential to validate the scheme's effectiveness outside of controlled environments. Pilot projects in urban settings can provide valuable insights into the system's performance in real traffic conditions and user acceptance.
7. **Sustainability and Environmental Impact:** Future research should also consider the environmental impact of implementing such technologies in smart cities. This includes assessing the energy efficiency of the communication systems and exploring ways to minimize the carbon footprint of vehicular networks.

In conclusion, while the proposed scheme demonstrates significant potential in enhancing vehicular communication security using blockchain technology, these recommendations aim to guide future research toward addressing scalability, security, economic, and environmental considerations for more holistic development and implementation.

# References

- [1] G. Zhong and X. Gu, “Design and research of intra cluster routing protocol for vehicle ad hoc networks,” in *2022 3rd International Conference on Computer Science and Management Technology (ICCSMT)*, 2022, pp. 322–325.
- [2] T. A. Sohan, H. H. Haque, M. A. Hasan, and M. J. Islam, “Investigating the challenges of dynamic spectrum access in cognitive radio-enabled vehicular ad hoc networks (cr-vanets),” in *2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, 2015, pp. 1–6.
- [3] H. Mhamdi, A. Zouinkhi, and H. Sakli, “Smart contracts for decentralized vehicle services,” in *2021 International Wireless Communications and Mobile Computing (IWCMC)*, 2021, pp. 1846–1851.
- [4] N. Kalaivani, R. Raman, C. C. S. Basavaraddi, V. Kumar Pandey, and S. Sangeetha, “Enhancing air travel with iot: Smart airports and passenger experience,” in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 2023, pp. 1300–1305.
- [5] S. Deb, D. W. Carruth, and C. R. Hudson, “How communicating features can help pedestrian safety in the presence of self-driving vehicles: Virtual reality experiment,” *IEEE Transactions on Human-Machine Systems*, vol. 50, no. 2, pp. 176–186, 2020.
- [6] Y. Wang, L. Yuan, W. Jiao, Y. Qiang, J. Zhao, Q. Yang, and K. Li, “A fast and secured vehicle-to-vehicle energy trading based on blockchain consensus in the internet of electric vehicles,” *IEEE Transactions on Vehicular Technology*, vol. 72, no. 6, pp. 7827–7843, 2023.
- [7] A. Janarthanan and V. Vidhusha, “Cycle-consistent generative adversarial network and crypto hash signature token-based block chain technology for data aggregation with secured routing in wireless sensor networks,” *International Journal of Communication Systems*, vol. 37, no. 4, p. e5675, 2024. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.5675>

- [8] H. Ghafoor and I. Koo, “Cr-sdvn: A cognitive routing protocol for software-defined vehicular networks,” *IEEE Sensors Journal*, vol. 18, no. 4, pp. 1761–1772, 2018.
- [9] Q. Zhang, H. Zheng, J. Lan, J. An, and H. Peng, “An autonomous information collection and dissemination model for large-scale urban road networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1085–1095, 2016.
- [10] S. Namane, M. Ahmim, A. Kondoro, and I. B. Dhaou, “Blockchain-based authentication scheme for collaborative traffic light systems using fog computing,” *Electronics*, vol. 12, no. 2, 2023. [Online]. Available: <https://www.mdpi.com/2079-9292/12/2/431>
- [11] O. M. Khodayer Al-Dulaimi, M. K. Hassan Al-Dulaimi, and A. M. Khodayer Al-Dulaimi, “Cognitive radio technologies and applications in dynamic spectrum access method,” in *2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC ST)*, 2022, pp. 9–14.
- [12] M. Vološin, E. Šlapak, Z. Becvar, T. Maksymyuk, A. Petík, M. Liyanage, and J. Gazda, “Blockchain-based route selection with allocation of radio and computing resources for connected autonomous vehicles,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 7, pp. 7230–7243, 2023.
- [13] G. Rathee, F. Ahmad, F. Kurugollu, M. A. Azad, R. Iqbal, and M. Imran, “Crt-biov: A cognitive radio technique for blockchain-enabled internet of vehicles,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4005–4015, 2021.
- [14] H. Chang, Y. Liu, and Z. Sheng, “Blockchain-enabled online traffic congestion duration prediction in cognitive internet of vehicles,” *IEEE Internet of Things Journal*, vol. 9, no. 24, pp. 25 612–25 625, 2022.
- [15] S. Akter, M. S. Rahman, M. Z. A. Bhuiyan, and N. Mansoor, “Towards secure communication in cr-vanets through a trust-based routing protocol,” in *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2021, pp. 1–6.
- [16] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, W. Mansoor, and U. Biswas, “Design of a blockchain enabled secure vehicle-to-vehicle communication system,” in *2021 4th International Conference on Signal Processing and Information Security (ICSPIS)*, 2021, pp. 29–32.
- [17] E. M. Ghourab, L. Bariah, S. Muhaidat, P. C. Sofotasios, M. Al-Qutayri, and E. Damiani, “Reputation-aware relay selection with opportunistic spectrum

- access: A blockchain approach,” *IEEE Open Journal of Vehicular Technology*, vol. 4, pp. 389–403, 2023.
- [18] H. Sohail, M. u. Hassan, M. A. Elmagzoub, A. Rajab, K. Rajab, A. Ahmed, A. Shaikh, A. Ali, and H. Jamil, “Bbsf: Blockchain-based secure weather forecasting information through routing protocol in vanet,” *Sensors*, vol. 23, no. 11, 2023. [Online]. Available: <https://www.mdpi.com/1424-8220/23/11/5259>
- [19] Y. Park, C. Sur, K.-H. Rhee, and I. You, “A secure incentive scheme for vehicular delay tolerant networks using cryptocurrency,” *Sec. and Commun. Netw.*, vol. 2018, jan 2018. [Online]. Available: <https://doi.org/10.1155/2018/5932183>
- [20] R. Jabbar, N. Fetais, M. Kharbeche, M. Krichen, K. Barkaoui, and M. Shinoy, “Blockchain for the internet of vehicles: How to use blockchain to secure vehicle-to-everything (v2x) communication and payment?” *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15 807–15 823, 2021.
- [21] E. K. Subramanian, M. Rajkumar, T. Poovizhi, and S. K. Mohapatra, “Group shared mobility platform activated via blockchain,” in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, 2023, pp. 689–693.
- [22] W. Ahmed, W. Di, and D. Mukathe, “Blockchain-assisted privacy-preserving and context-aware trust management framework for secure communications in vanets,” *Sensors*, vol. 23, no. 12, 2023. [Online]. Available: <https://www.mdpi.com/1424-8220/23/12/5766>