Vehicular Communications 31 (2021) 100386

Contents lists available at ScienceDirect

Vehicular Communications

www.elsevier.com/locate/vehcom

Futuristic blockchain based scalable and cost-effective 5G vehicular network architecture

Usama Arshad *, Munam Ali Shah, Nadeem Javaid

COMSATS University Islamabad, Islamabad 44000, Pakistan

ARTICLE INFO

Article history:
Received 17 December 2020
Received in revised form 3 June 2021
Accepted 28 June 2021
Available online 3 July 2021

Keywords:
Blockchain
IoT
5G
Scalability
ITS
Vehicular network architecture

ABSTRACT

In the present era, smart and efficient vehicular network architectures are necessary due to fast technological advancements in vehicles. Many problems arise in these complex networks, which can be handled using blockchain and the Internet of Things (IoT). We proposed a comprehensive blockchain based 5G vehicular network architecture, which is cost-effective, scalable, secure, and handles various vehicular network issues in a smart city. The proposed architecture consists of all essential components like reputation system, incentive mechanism, and priority based techniques to handle different limitations in the literature. Simulations results for different scenarios depict the high execution cost of a single controller node, minor node, and ordinary node as 106305, 85864, and 65491 gas values and transaction cost as 130521, 109824, and 89195 gas values. The results depict the effectiveness of the proposed architecture in terms of scalability, time and cost-effectiveness.

1. Introduction

In the present era, most of the population lives in urban areas to lead an easy life away from rural life's hardships. The technology in the present era is making lives easier, and with each passing day, we witness a new change in our cities and daily lives [1]. People are moving towards cities, especially smart cities. As these cities offer high quality of life, so in the future, all cities in the world will be made smart. As the population is growing rapidly, we need such smart cities that are sustainable on their own. Smart cities provide a sense of security and ease; however, many problems also arise in a smart city like handling a huge population and their data, privacy, security, scalability, and adaptability. Smart cities are a collection of different smart networks working with each other or separately in the city. These networks provide daily services to fulfill the needs of the population. From smart grids for low energy consumption to secure vehicular networks, technology is progressing rapidly, and the world is changing faster than we can imagine. This change is only possible thanks to the advancements in technologies like Artificial Intelligence (AI) and blockchain. Many other fields that help revolutionize the world are also changing at a great pace [2]. As these fields grow and change, many discoveries and inventions happen that make our lives easier and faster. To overcome the problems in smart cities and smart networks, various models are proposed by researchers. Traditional vehicular networks are unable to provide security and are certainly unable to handle smart vehicles. We need smart networks to handle smart devices. In smart vehicular networks, technologies like the Global Positioning System (GPS) are used. These technologies help to locate vehicles.

However, now with electric vehicles, different kinds of onboard resources like sensors, storage devices, radars, cameras, Event Data Recorders (EDR) etc., are used to perform different actions [3]. All of these devices collect big data to perform their actions, and they have to share limited data in the network to increase the throughput and work effectively [4]. Using all these resources, devices and networks become aware of the environment and conditions. This helps in increasing their overall effectiveness and performance [5]. In the present era, the human population is highly dependent upon smart devices. As smart devices make our lives easier, many problems arise due to these smart devices. The main issues that arise from these smart devices include lack of security, and privacy [6], [7]. Data is considered expensive in this era, and people want to protect it because data in the wrong hands can be dangerous. In smart networks, different nodes work together and share data. However, as all network nodes are strangers to each other, it creates an environment with a lack of trust. Different vehicles share valuable data in the vehicular network like traffic conditions in an area.

Moreover, these vehicular networks have limited devices to store and share data. It is impossible to store this data on these

* Corresponding author.
E-mail addresses: usamajanjua9@gmail.com (U. Arshad), mshah@comsats.edu.pk (M. Ali Shah), nadeemjavaidqau@gmail.com (N. Javaid).

https://doi.org/10.1016/j.vehcom.2021.100386
2214-2096/

small devices. This problem is solved by using Road Side Units (RSU) [8]. These RSUs save all the data collected by vehicles and provide limited amount of data when required. Sharing resources with other nodes in a network is also a problem. Due to this, some nodes may act selfishly in the network. Trust management can be done by sharing required resources as needed. Different techniques are proposed for this purpose [9]. Apart from simple trust management, many incentive mechanisms are proposed based on data sharing and storage management [10]. Other incentive mechanisms are proposed based on data stored by nodes to promote data storage in nodes. Incentive mechanisms are used to decrease or eliminate the selfishness of nodes in the networks. Nodes need to communicate faster in a network to work effectively. In [11], [12], the authors proposed techniques for providing safe computing services to the lightweight clients on the blockchain. The models provide a partially connected and fully connected blockchain concepts. Privacy, security, and a trustless environment are achieved using blockchain. Robustness and flexibility are also needed in networks as nodes may be far away from each other. This leads to nodes' failure, and to avoid these failures, many new techniques are proposed using trust factors. The trust factor is an amazing concept to solve many problems in the network. Each node is rated positive or negative after every action in the network. Apart from different blockchain based models, multi-blockchain models are also proposed over time. In [13], the authors proposed a blockchain based model with two blockchains. One blockchain is used to detect fraud users and the other is used to check integrity. Convolutional Neural Networks (CNN) are also used to authenticate nodes. However, this kind of model is limited in terms of scalability and with increasing size, these models do not remain cost-effective. This reputation system helps to eradicate the selfishness of nodes and improve the overall performance of the network. Hence, many issues can be solved by using different techniques and methods.

1.1. Blockchain

Blockchain is the best technology for the present age. It is a decentralized and distributed ledger. Due to this distributed approach, it is also called a distributed ledger technology. Blockchain is an old concept, but it became popular in 2008 when Bitcoin came in front of people and revolutionized the concept of currency worldwide. It is a distributed and decentralized currency, which had no single owner like other currencies. With time, people realized that blockchain technology could be used for many different applications. In simple words, we can take blockchain as a google doc that is shared with a group of people. This document is not copied by all the people but only shared by all at the same time. The next big thing that blockchain has is cryptographic hashing. After the blockchain came to the surface in 2008, many new technologies like holochain also emerged following the same concepts. Just like any other technology, blockchain also consists of many components. Each component is getting updated with time. Blockchain eradicated the need for third-party in all kinds of transactions and provided a high level of security and privacy that was not possible before.

The three main components of blockchain are block, miners, and nodes. The transaction data is stored in blockchain. The number of blocks in blockchain is not fixed, and each block consists of three main things, nonce, data, and hash (see Fig. 1). A nonce is a whole number that is changed every time data is changed. Hash is joined with this nonce, which helps to secure blockchain. Whenever a new block is added, it is done by the process of mining. Mining is the process in which miners solve a complex mathematical problem to find the nonce, and this nonce provides a hash, which is accepted. This process needs high computational power,

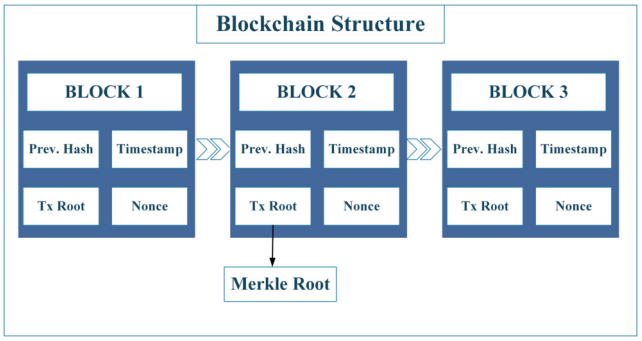

Fig. 1. Blockchain Structure.

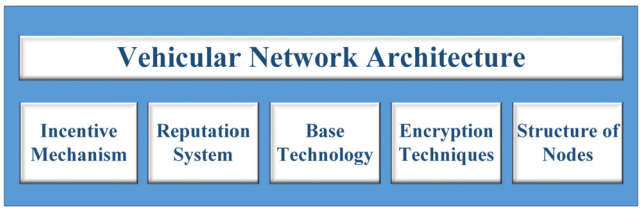

Fig. 2. Main Components of Vehicular Network Architecture.

making it difficult for hackers to hack the blockchain. The first block in any blockchain is called genesis block, and as the number of nodes increases in a blockchain, it becomes more and more secure due to its distributed nature. Nodes in blockchain join to form a network, and for every update in blockchain, the majority of nodes approve the actions. This process is called the consensus mechanism, and with time, researchers have proposed many new consensus mechanisms for different techniques and uses of blockchain technology. Some of the most used consensus mechanisms include Proof of Work (PoW), Proof of Authority (PoA), and Proof of Concept (PoC). Smart contracts and tokens are used with blockchain technology to achieve transactions without any kind of involvement of third parties.

1.2. Blockchain based vehicular network architectures

Blockchain based networks are the new future due to the distributed approach of blockchain technology. Intelligent Traffic System (ITS) is becoming better with the use of the latest technologies. These networks have to handle the latest auto-driving vehicles, which are smart and consist of the latest technologies. Blockchain based vehicular network architectures are the best to handle these smart vehicles. Much research is done on vehicular networks and different components of blockchain based networks.

Blockchain based vehicular network architecture consists of different components, and each of these components solves a particular problem in such networks. With these technologically advanced vehicles, we need smart networks to handle big data and smart tasks like fast information sharing. Many problems arise in these complex networks, like scalability, cost-effectiveness, adaptability, nodes' selfishness, malicious nodes, security, and privacy, which can be handled using blockchain and the Internet of Things (IoT).

Many vehicular network architectures are proposed in the literature, and each component of this architecture is also proposed separately to handle a particular problem. The main components of vehicular network architecture are given below (also see Fig. 2):

- Incentive Mechanism
- Reputation System
- Base Technology
- Encryption Techniques

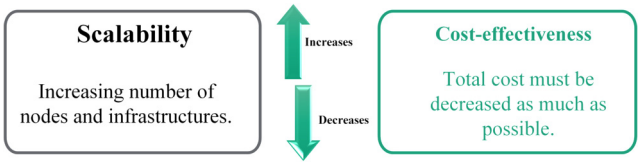

Fig. 3. Scalability Vs Cost.

- Structure of Nodes

Each component is necessary to perform a particular task and the number of components can increase or decrease according to the scenario.

1.3. Scalability vs cost

With technological advancements, infrastructure is getting more costly, thus, increasing the deployment and execution cost. Moreover, scalability is not achievable without sacrificing execution cost, according to the literature review. Scalability is achieved with the deployment of costly infrastructure. Scalability and cost-effectiveness are inversely proportional in vehicular network architectures proposed in the literature. Fig. 3 clearly depicts the relation between scalability and cost-effectiveness.

1.4. 5G and deployment issues

5G is the latest technology, and like all technological advancements, 5G infrastructure is costly. Moreover, 5G technology has a high frequency of waves that can not be penetrated through walls easily and needs a lot more infrastructure than 4G. 5G deployment itself faces many issues, and much work is done to handle all its issues separately. Some main deployment issues are shown in Fig. 4.

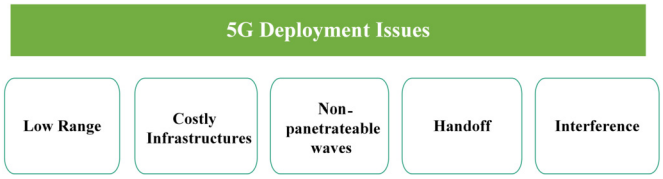

Fig. 4. 5G Deployment Issues.

Table 1
List of Abbreviations.

Abbreviation	Explanation
ADVs	Auto Driving Vehicles
AI	Artificial Intelligence
CNN	Convolutional Neural Network
EDR	Event Data Recorders
EVs	Electric Vehicles
GPS	Global Positioning System
IoT	Internet of Things
ITS	Intelligent Traffic System
LoS	Line-of-Sight
MIMO	Multi-Input Multi-Output
NLoS	Non-Line-of-Sight
PoA	Proof of Authority
PoE	Proof of Event
PoW	Proof of Work
RSU	Road Side Unit
VNA	Vehicular Network Authority
PoC	Proof of Concept
VANET	Vehicular Ad-hoc Network
MANET	Mobile Ad-hoc Network
ISP	Internet Service Provider
C-CHAIN	Controller Blockchain
O-Chain	Ordinary Blockchain
R-Chain	Repairing Blockchain
Med-Chain	Medical Blockchain
AES	Advanced Encryption Standard
DES	Data Encryption Standard

1.5. Background of 5G issues

As electric vehicles replace normal vehicles in a smart city, we also need advanced smart networks to handle these smart vehicles. Many technological advancements like blockchain, the Internet of Things (IoT) and latest communication technologies like 5G play an important role in providing solutions to the modern problems. The authors in [14] described the different present and future trends for the 5G network. The authors described in detail the costly infrastructure of 5G and the deployment trends around the world. The conducted survey clearly depicts that most of the developed world will deploy 5G by 2022. However, an underdeveloped world like Asia may take up to 2025 to deploy 5G. The main goal of the 5G technology is to achieve high data rates of 100 Mbps to 1 Gbps for everyone around the world anytime, anywhere. However, the deployment of such technology is not easy. To achieve these data rates, different technologies like small cell networks [15], Massive Multi-Input Multi-Output (MIMO) [16], and millimeter wave [17] are used. When we look at an example of 5G deployments, like Samsung's prototype model [18], we can see that their prototype is providing a data rate up to 1 Gbps. However, this model is also facing the issue of distance. The model is operating at a frequency of 27.925 GHz at a distance of 1.7 kilometers. However, this 1.7 kilometers connectivity is only in the Line-of-Sight (LoS) transmission. When it comes to Non-Line-of-Sight (NLoS) transmissions, it only operates over the range of 200 m. 5G network started with the technology of millimeter wave. However, as 5G has high frequency and short wavelengths when transmitted over milliliter wave technology, link distance is reduced. After the millimeter wave, the trend of small cells started [19]. Small cells provide the availability of networks in short ranges, with the capability to switch between different small cells. In different proposed models, small cells are used with already available infrastructures to provide cost-effective 5G infrastructure. Apart from cost-effective infrastructure, much work is being done to improve connectivity and coverage of the 5G network. The authors in [20] described the thorough analysis of coverage for 5G networks based on small cell networks. A multi-directional path loss model is proposed to handle the coverage of 5G small cell networks.

The authors in [21] discussed the 5G heterogeneous networks. The cost optimization, coverage, and handoff analysis are discussed in detail. Different technologies are joined together in 5G heterogeneous networks to provide coverage and performance to handoff. LoS and NLoS (A list of abbreviations and their meaning is provided in Table 1) scenarios are also discussed in detail. Many other issues like inter-cell and intra-cell interference occur in small cell 5G networks. The authors in [22] proposed different enabling techniques that include coordinated scheduling, multipoint scheduling, and inter-cell interference coordination to handle the issues related to interference management in 5G deployment of small cell networks. The authors in [23] chronologically described different interference issues in 5G networks and how they are solved using different techniques. The authors in [24] also proposed a technique to use the already available infrastructure instead of deploying a new costly infrastructure. The authors proposed the technique of using light poles to cover more areas in densely populated areas. However, this technique also needs investments to cover the deployment costs. So far, the main issues incurred in the existing research include the high-cost infrastructures, short-range connectivity, interferences, and handoff.

Research contributions

The main contribution of this research work is to achieve a high level of scalability in a blockchain based vehicular network architecture without sacrificing cost-effectiveness. This comprehensively proposed vehicular network architecture contributes to the literature that will act as a generic base research work for future in-depth research on all of its different components. The proposed model achieves better access management of nodes with priority based access management techniques to save the extra cost. The proposed model contributes to saving the vehicular network from unnecessary complexities, which consume more power, storage and increase the total execution cost. Different components are joined together to handle some of the known issues in blockchain based vehicular network architectures like selfishness of nodes, security, privacy and failure of nodes in one complete structure keeping in mind the cost-effectiveness and adaptability with future technologies.

2. Related work

The blockchain and IoT industry are developing rapidly and making our lives easier. Computer servers are used widely to store data and provide services as needed [25]. These services may be malicious and can cause damage to devices or the network. Authentication of services is also a problem faced in networks. Different kinds of consensus mechanisms are used in blockchain based networks to work efficiently. Many mechanisms are already provided to handle smart devices in networks. However, most of such mechanisms need high computational power and heavy resources. IoT devices are becoming normal, and it is important to create efficient mechanisms to handle such devices. The main goal is to effectively handle devices with less computational power and low resources without reducing network efficiency. A consortium blockchain is normally used with IoT devices, and the Proof of Authority (PoA) consensus mechanism is used for the effective working of networks. Edge service providers provide services, which may not be secure for the users. To handle this issue, Blockchain based models are used [26].

Similarly, consensus mechanisms like PoA are used with different types of blockchain. Apart from this, the new concept of off-chain is proposed in which services can be authenticated and identified easily. Huge networks also face latency. Blockchain based networks solve many such issues related to privacy, security, and identification. Many reputation systems are also proposed to handle nodes in the network. Moreover, blockchain based models also work effectively with IoT devices because of their peer-to-peer connection. Two devices in a network, directly connect with each other without any involvement of a third party. Another problem in traditional networks is access control of devices. Many proposed models handle access control in the network using different algorithms [27].

When we look at traditional models, they always have a third party between two entities. Blockchain based models remove most of these traditional problems. In blockchain models, all devices share data in a trust-less environment. Peer-to-peer connection in these models ensures direct communication. Hence, models are most secured and privacy based. The authors in [28] proposed a model on the blockchain which provides an incentive mechanism to nodes on the basis of data stored by them. Location and privacy leakage of users is a big problem, and users are reluctant to share information. The authors in [29] proposed a technique of blockchain based incentive mechanism. The authors in [30] proposed rating system and the concept of trust points to handle the malicious behavior of nodes. ITS uses ad-hoc networks to communicate in a vehicular network, which are not secure for data transmission. The protocols used in ITS are mostly not up to date, and work is being done to provide better security mechanisms. The authors in [31] proposed a consensus mechanism based on Proof of Event (PoE) rather than PoW or PoA concepts to handle the sharing of traffic data and its authenticity. The authors in [32] proposed IoT e-business model. The traditional model and the IoT e-business model are discussed and compared in detail. Smart property [33] and paid data are used as commodities in the proposed model. Moreover, it is explained how different nodes are interacting in the network. Table 2, clearly describes different proposed techniques and models for blockchain based networks, especially blockchain based vehicular networks. It also describes different deployment issues of 5G and work done by different authors with possible limitations. Our proposed model handles limitations in old models.

The authors in [34] proposed a blockchain based Healthcare system, which handles data storage of patients' data. Patient-driven interoperability and institution-based interoperability is an issue for a long time. Institution-based and patient-based interoperability is discussed in detail with possible solutions. Privacy leakage through unique ids can be a problem for patients [35].

Much work is done by researchers on privacy-preserving and priority-based techniques. The use of vehicular ad-hoc networks has brought a revolution to achieve traffic safety. The authors in [36] proposed an authentication scheme that is weight-based. They used weights to control the malicious vehicles in the network and gave priority to the vehicles on the basis of the weight assigned to them. To secure the communication between the vehicles, they used a conditional privacy-preserving scheme. Their proposed model decreases the total costs using the SDN and priority approach. In [37] authors discussed different challenges related to privacy and security in 5G enabled vehicular networks. The research mainly focused on the infrastructure and case study to ensure the privacy and security challenges. A 5G enabled infrastructure is proposed for vehicular networks. However, this model lacks a solution to some of the known issues like scalability and adaptability. Finding charging stations and security connecting with others is a challenge with electric vehicles, and many infrastructures are proposed in the literature to ensure security and privacy for electric vehicles. The authors in [38] proposed a secure framework for electric vehicles, which is privacy-preserving. Cryptography is used to ensure security and privacy. The model performs well in terms of communication costs and satisfaction ratio. The performance of the model is also compared with recently published research. The authors in [39] discussed in detail about the security, privacy, and trust management in blockchain based solutions. They have surveyed different recently published researches to review and classify different issues and solutions proposed.

The authors in [41] proposed detailed scenarios and discussed 5G network and infrastructure scenarios in detail. They proposed that instead of developing the new 5G infrastructure, we should use already developed infrastructures. Due to high infrastructure costs, different models are proposed to use the existing infrastructure for 5G instead of creating new infrastructures from scratch. The authors in [42] proposed techniques to handle issues like low storage and high complexity. The high complexity problem of data storage in the blockchain is addressed. Provided blockchain based method to store more data on nodes with less complexity. However, the model can be easily compromised, as data is stored in fewer nodes. The authors in [43] show how data can be secured on fog or cloud computing with the proposed framework and how it can be saved from different attacks. The authors in [44] proposed blockchain based distributed vehicular network architecture and performance analysis. Problems like security, scalability, big data storage, and privacy in a vehicular network are discussed in detail. Management of big data in vehicular networks while providing privacy, adaptability, and security is also discussed. However, traffic

Table 2
Proposed Solutions in Literature.

Proposed Model	Experimentation	Problem Addressed	Contribution	Limitation
Proposed model to provide safe security services on blockchain. [11]	Etherium environment is used.	Malicious services provided by edge servers to clients.	Privacy, security, and a trustless environment are achieved using blockchain.	Latency in large networks.
Proposed blockchain based user access strategies for D2D networks. [13]	A CNN is used for the prediction of fake users.	Detection of fraud users.	User access based on consensus mechanism is proposed using blockchain	It is limited in terms of scalability.
A detailed survey on 5G deployment is carried out and future trends are discussed. [14]	Data is collected from 46 different chief technology officers.	The hype about the 5G network. No graphical representation depicts different scenarios.	Collected all data from around the globe to show the trends and development of 5G networks.	The survey is limited in terms of data collected as it is collected from only 46 chief technology officers. New proposed techniques can change the shown trends.
A multi-directional path loss model is proposed to handle the coverage of 5G small cell networks. [15]	Simulations show the improvement of path loss and coverage issues.	Short distance coverage and handoff issue of 5G small cell networks.	Solved the issue of path loss in 5G small cell networks. Handled issues of coverage and handoff.	Path loss is handled while network coverage still has a short distance.
Proposed techniques for cost optimization, coverage, and handoff analysis. [16]	Different scenarios are represented with stats and calculations. The hypothesis is used to produce results.	Coverage, handoff, cost optimization in heterogeneous 5G networks.	Different technologies joined together in 5G heterogeneous networks to provide coverage and performance to handoff. LoS and NLoS scenarios are also discussed.	A different hypothesis is used to produce results. Results may not be the same in actual scenarios.
Proposed and reviewed techniques to handle issues related to interference management in 5G networks. [17]	Visual representation of different scenarios and review of the research challenges.	Interference management in 5G networks.	Proposed coordinated scheduling, multipoint scheduling, and inter-cell interference coordination to handle the issues related to interference management.	Solutions may be limited in terms of scalability.
The proposed technique of using the present infrastructure for 5G networks. [24]	Different simulations represent the scenarios of 5G networks.	Costly 5G infrastructure.	The proposed technique of using light poles as 5G infrastructure to reduce the cost of infrastructure deployment.	Investments may not be available for proposed deployment.
Proposed blockchain based trust mechanism to detect malicious nodes in the network. [30]	Windows 10 operating system with a specification of Core i7 and 16 GB ram is used. Python is used for implementation.	Detection of malicious nodes in the vehicular network.	Branch-based blockchain technology in intelligent vehicles. Branch-based blockchain for vehicular networks.	A decentralized approach may not be feasible for a trust mechanism.
Proposed blockchain based Healthcare system, which handles storage of patients' data. [34]	The model can be implemented in a Remix or Ethereum environment.	Patient driven interoperability and institution-based interoperability.	Institution-based and patient-based interoperability is discussed.	Privacy leakage through unique ids.
Blockchain based network coded distributed storage technology is proposed with less complexity. [42]	The model is analyzed based on storage, consensus speed, etc.	Low storage and high complexity problems in the blockchain.	Provided blockchain based method to store more data on nodes with less complexity.	The model can be easily compromised as data is stored in fewer nodes.

between vehicles is not covered, and the non-reliability of channels in any cellular network also create issues.

In our recent work [45], we proposed a blockchain based vehicular network architecture that was scalable, robust, and adaptable by using vehicular network architecture similar to proposed in [46] with a rating system similar to proposed in [47] to handle malicious nodes. However, after achieving scalability, vehicular network architecture lost its cost-effectiveness and executive effectiveness. Fig. 5 clearly describes our recent blockchain based vehicular network architecture. The goal is to achieve a high level of scalability without sacrificing execution efficiency and cost-effectiveness. Moreover, after the inclusion of 5G, many features may change in vehicular networks [48]. However, our proposed system will work perfectly in a 5G based environment. Due to the high frequency of the 5G network and shorter range, we need more infrastructure to build, which increases the total cost of vehicular networks. Our model provides the best solution in this case for scalability and performance. We solved the limitations of our recent work with the new proposed model and the system's modifications. Simulations and results clearly describe the effectiveness of modified vehicular network architecture. Passenger's health care is also explained in detail and how passengers' safety and health can be insured in a smart city. Node failure and malicious nodes are handled more effectively with the proposed incentive mechanism. Table 3 describes different blockchain based proposed models with possible limitations.

3. Problem statement

Blockchain based vehicular network architectures have been proposed in [45], [47], which provide scalability, robustness and can handle malicious nodes. However, using blockchain in this type of network scenario imposes a high computational cost and is time-consuming. Moreover, due to the costly infrastructure of the latest technologies like 5G [41], and deployment issues [14], [16], a cost-effective and scalable vehicular network architecture is needed. The decentralized mechanism used for achieving privacy and security adds to the computational cost. Thus, making

Table 3
The motivation of proposed research.

Proposed Model	Experimentation	Problem Addressed	Contribution	Limitation
Blockchain based trust management system is proposed. [40]	Python and Go-language environment.	Privacy preserving was not achieved in vehicular networks.	Trust management is achieved without exposing vehicles to other vehicles.	Complex model limited in terms of speed and time.
Proposed that use of already present Infrastructure can help to save infrastructure development cost. [41]	Different data from different scenarios are plotted on a graph to show the difference between old models and the proposed model.	High cost of infrastructure for future and present technologies like 5G.	Complete research work to decrease the 5G infrastructure cost using already present infrastructure.	Limited scenarios are discussed with controlled variables. Our work is motivated by the proposed work.
Proposed blockchain based distributed vehicular network architecture and performance analysis. [44]	MATLAB tool is used for simulations.	Security, scalability, big data storage, privacy.	Proposed blockchain based vehicular network architecture with five blockchains.	Network traffic scenarios between vehicles is not covered, and the reliability of channels in any cellular network can also create issues.
Blockchain based vehicular network architecture and trust management system is proposed. [45]	Ethereum and Remix are used to represent node activities and performance.	No general vehicular network architecture, which can handle most of the known issues.	Complete vehicular network architecture and solution to its possible limitations.	Execution time and cost increases with increasing scalability.
Blockchain based trust management system is proposed. [47]	Simulations are done on MATLAB.	No proper blockchain based decentralized trust management was proposed.	Trust management system, which is decentralized using blockchain.	No broad scope of work and system is limited in terms of scalability.

Table 4
Comparison with Other Models.

Ref No.	Blockchain Technology	Privacy	Security	Scalability	Adaptability	Cost-effectiveness
[45]	✓	✓	✓			
[47]	✓			✓	✓	✓
[40]	✓	✓	✓			
[41]	✓	✓	✓			
Our Proposed Model	✓	✓	✓	✓	✓	✓

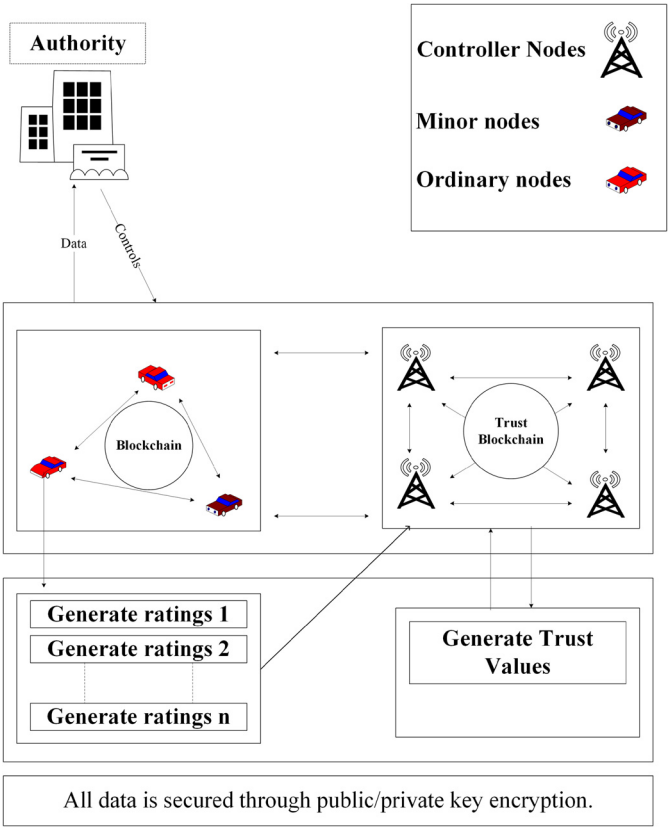

Fig. 5. Old Proposed Blockchain based Vehicular Network Architecture.

the systems less efficient [40]. There is a need to improve the existing architectures in terms of high computational cost and low efficiency. Table 4 depicts the availability of technology and features in different existing proposed approaches and our proposed approach.

4. Proposed model

We proposed a scalable blockchain based 5G vehicular network architecture in a smart city and a solution to possible limitations in blockchain based networks in a smart city necessary for the vehicular network to work effectively. The main limitations handled by our proposed model include privacy, security and scalability without sacrificing efficiency, cost, node failure, health emergencies, and selfishness of nodes. Our proposed vehicular network architecture consists of three kinds of nodes and one Vehicular Network Authority (VNA). The kinds of nodes are as follows:

- Ordinary nodes
- Controller nodes
- Minor nodes

Ordinary nodes. Ordinary nodes are vehicles with less computational and execution power. These nodes request data and services from controller nodes. Due to less storage these nodes cannot store big data. Hence, they request only a limited amount of necessary data from the controller nodes.

Controller nodes. Controller nodes are fixed nodes and are known as Road Side Units (RSUs). These nodes have high computational and execution power. Controller nodes store huge amount of data on them and provide services to other nodes.

Minor nodes. Minor nodes are vehicles with good computational and execution power. They act as a bridge between controller

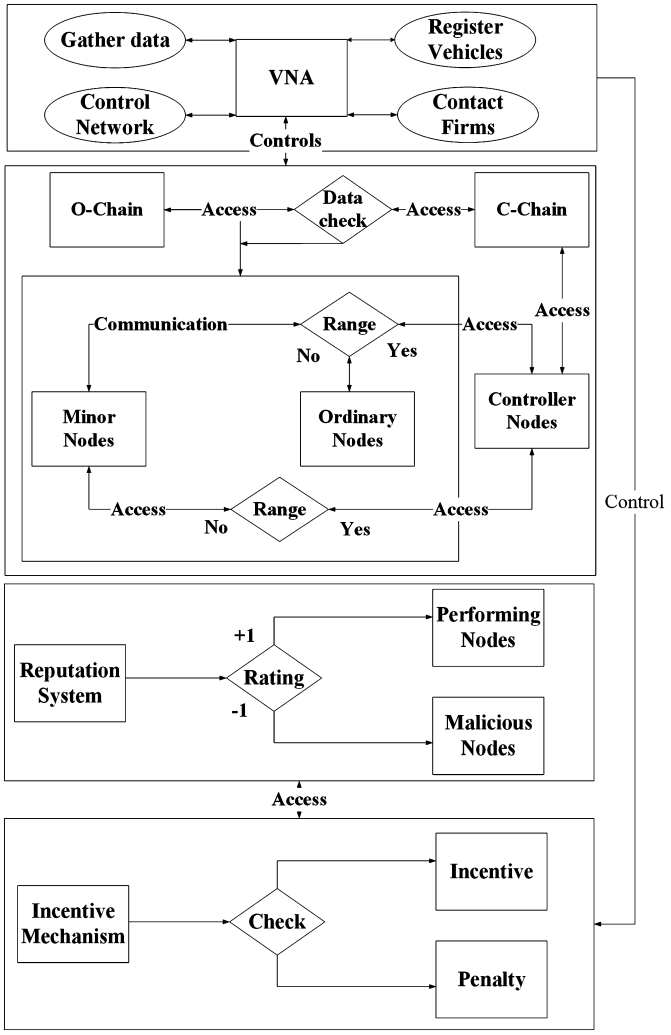

Fig. 6. Flowchart Diagram of Proposed Model.

nodes and ordinary nodes if nodes are far away from each other. Nodes are registered as minor nodes in the network based on their storage, execution, and computational power.

Vehicular Network Authority (VNA). A vehicular network authority also exists in the proposed model. The authority registers all nodes and handles any failure that occurs in the network. On registration, vehicles are granted the status of minor node or ordinary node depending on their computational and execution resources. VNA can add or remove any node from the vehicular network based on its reputation in the network. VNA acts as a controller of the whole vehicular network. VNA also handles the incentive provisioning mechanism based on the node's reputation. VNA has full control over the network and can make changes as needed in the network. In case of emergency or node failure, VNA contacts the respective services or en-route the vehicle to the closest services available. It is assumed that the VNA can never be compromised. Fig. 6 clearly represents the flow of our proposed model.

4.1. Proposed 5G Vehicular Network Architecture on Blockchain (5G-BLOCKVN)

We proposed a 5G vehicular network architecture based on the blockchain, which is scalable and adaptable. Apart from 5G, this architecture can work perfectly with any communication technology of the future without sacrificing cost and execution effectiveness. Three main nodes work together in the model under the

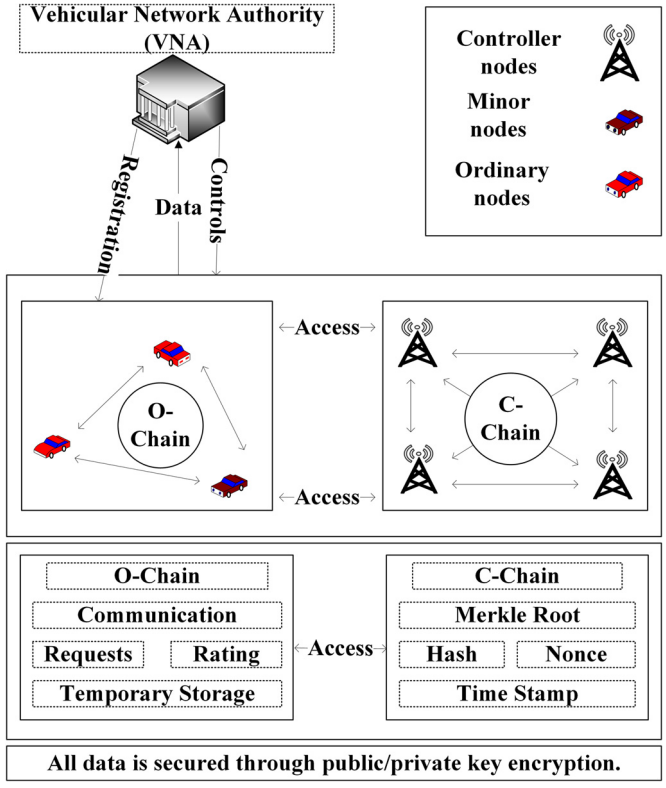

Fig. 7. Proposed 5G Vehicular Network Architecture on Blockchain (5G-BLOCKVN).

supervision of VNA. The vehicular network architecture consists of two blockchains. One blockchain is for controller nodes, which is called C-Chain. These nodes have to handle big data and without blockchain if these nodes are destroyed or damaged somehow, the data will be lost and the network will not work effectively.

Moreover, ordinary nodes and minor nodes cannot handle big data. Hence we cannot use the same blockchain with them. Minor nodes and ordinary nodes can request the services or data from controller nodes as needed. They have a separate blockchain termed as O-Chain to store temporary data needed at the time. O-Chain saves the data necessary for the services at a particular time and takes its data from C-Chain as needed. The minor nodes are the most important nodes in the model. As 5G requires a huge infrastructure to work effectively, which is costly. Hence, we introduced minor nodes for scalability. Ordinary nodes request controller nodes for the services, however, if they are out of range they will request from minor nodes and minor nodes will act as a bridge between controller nodes and ordinary nodes. Minor nodes can also request services from controller nodes as needed or from other minor nodes when no controller node is available in the range. This solves the problem of scalability, however, more number of minor nodes requesting each other can increase the overall cost and efficiency will be decreased as time will be increased to handle and response all requests of the network. To maintain efficiency, all nodes must perform their tasks efficiently in the network, which can be achieved by using incentive mechanism and reputation system. Fig. 7 clearly describes our proposed model.

4.2. Reputation system for 5G-BLOCKVN

In a vehicular network, all nodes communicate with each other and it is important for all them to act properly in the network. To avoid malicious behavior of nodes, we proposed a reputation system for nodes. Unlike other complex reputation systems that lack speed and accuracy, we proposed the simplest system with either a

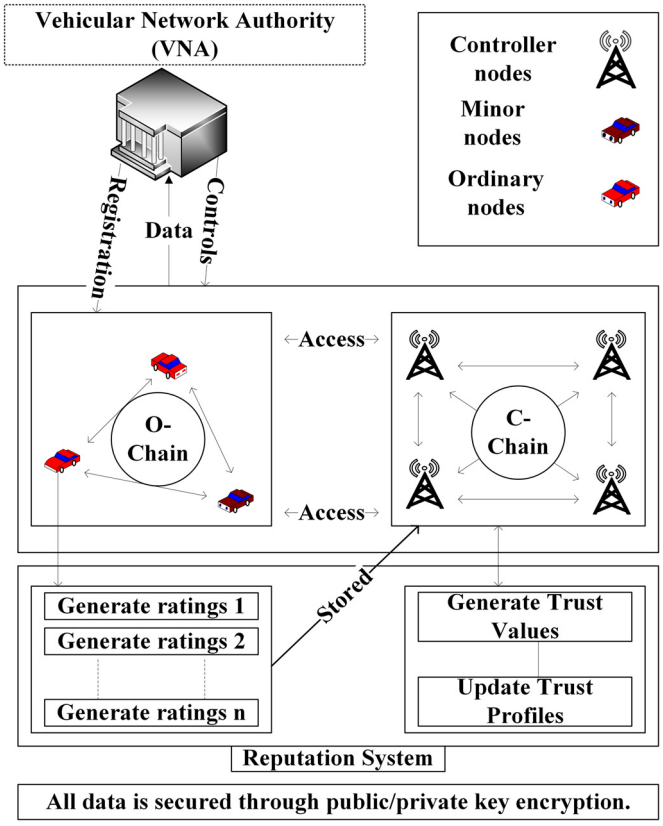

Fig. 8. Reputation System for 5G-BLOCKVN.

positive or negative rating. Minor nodes act as the bridge between all the nodes in the network hence they can show malicious behavior in the network. To increase the scalability they must work best in the network. To make sure these nodes work perfectly reputation system is necessary.

All nodes have their own profiles which can be seen before communication. Hence vehicles can request services from nodes which have good profiles. Whenever two vehicles communicate with each other, both rate each other either positively or negatively after communication. If the rating is positive, 1 is added to the profile and if the rating is negative, 1 is subtracted from the profile. Whenever a profile hits 0, the vehicle is removed from the network by VNA after checking the history of the profile. The history of the profile is checked to make sure that the profile is hitting 0 due to rapid negative ratings from other vehicles. In this way, the efficiency of the whole network is increased. Fig. 8 represents our proposed reputation system.

4.3. Incentive mechanism for 5G-BLOCKVN

Minor nodes have better storage, execution, and computational power than ordinary nodes. Hence, they may act selfishly in the network to save their resources. To control this selfishness of nodes, an incentive mechanism is proposed. As we already have a reputation system, we will use the data from the reputation system to reward or penalize nodes instead of a complex incentive mechanism. VNA will reward the controller nodes with good behavior on monthly or yearly and penalize on selfish behavior, respectively. Fig. 9 describes the proposed incentive mechanism in detail.

4.4. Priority based technique for 5G-BLOCKVN

Scalability can be achieved on the expense of cost-effectiveness. Nodes look for the closest node in range to communicate. This

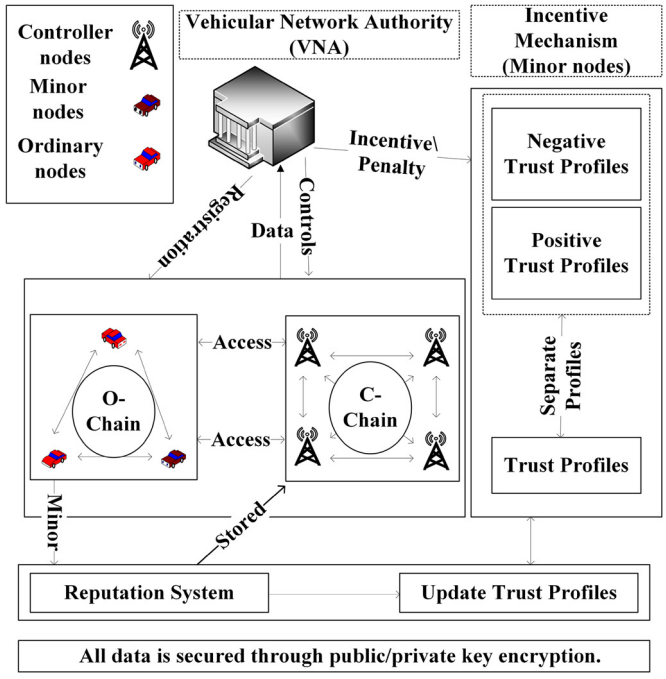

Fig. 9. Incentive Mechanism for 5G-BLOCKVN.

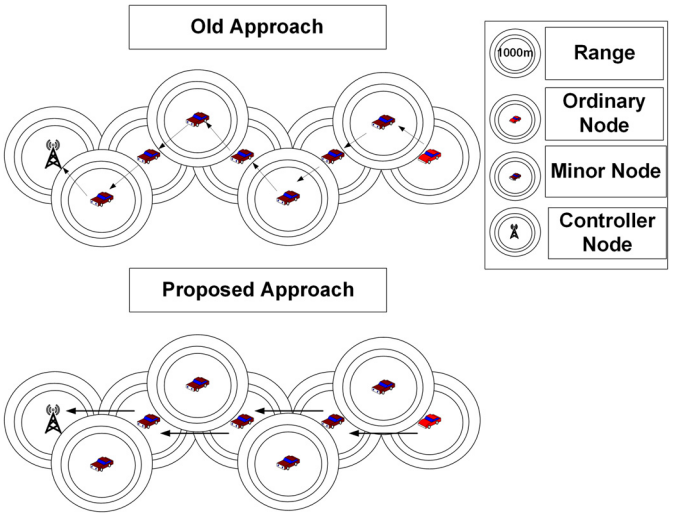

Fig. 10. Priority based Technique for 5G-BLOCKVN.

means too many minor nodes are involved in the network and each will have an executional cost and time delay. To handle this issue, we proposed priority based connections. Fig. 10 describes the old and new proposed approach. This priority of nodes can be shown by two main cases:

(1) CASE 1: Priority Based Ordinary Node Communication
(2) CASE 2: Priority Based Minor Node Communication

Fig. 11 clearly shows both the cases in detail.

4.4.1. Priority based ordinary node communication

In the case of an ordinary node, it should always look for the closest controller node in the network. However, if controller node is not available in the range then it must look for the most away minor node in range.

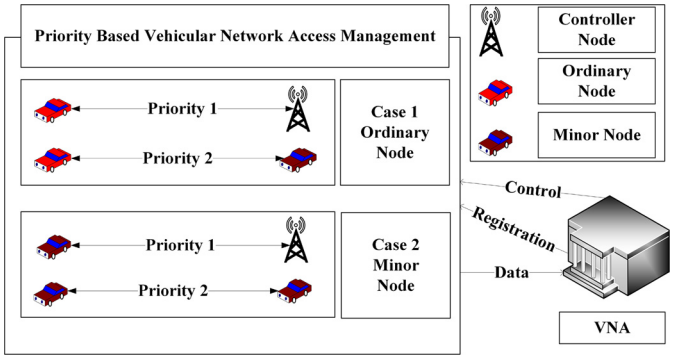

Fig. 11. Priority based Technique for 5G-BLOCKVN (Two Cases).

4.4.2. Priority based minor node communication

In the case of minor node, it should always look for the closest controller node in the network. However, if controller node is not available in the range then it must look for the most away minor node in range.

4.5. Privacy-preserving and security

Vehicles should only be identified by VNA and in case of reputation, the vehicle's privacy should be preserved. To tackle the problem of privacy leakage, instead of using some complex system, we simply used unique ids for ordinary nodes and minor nodes. This unique id consists of two parts: the first part consists of fixed unique numbers only known by VNA while the other part consists of randomly generated numbers. This randomly generated part changes automatically rapidly after an interval of time. This technique changes the id of every vehicle in the network continuously, which preserves privacy while keeping nodes known to VNA. When it comes to security, a high level of security can be achieved for communication using the latest encryption techniques.

4.6. Node failure and passenger healthcare

Node failure is the biggest issue in vehicular networks and this could be dangerous for the entire vehicular network. Due to the decentralized blockchain, no data is lost even if any node fails in any way. The basic failure of a node may include sensor failure or device failure. In such a case, VNA will automatically contact the closest repairing firm and share the location and repairing history of the vehicle with the firm. Repairing history is stored on a repairing blockchain called R-Chain. In case of any medical emergency in the vehicle, vehicles are automatic en-route to closest health services. Medical blockchain, called a Med-Chain, holds the data of patients, which can be accessed by the doctors only if patients allow them the access. Fig. 12 clearly represents node failure and passengers' healthcare.

4.7. 5G cost-effective infrastructure for 5G-BLOCKVN

Controller nodes are the main source points of the 5G network as part of the infrastructure. Using NLoS, we can achieve the range up to 1.7 km, and LoS can reach a range from 200 m to 1000 m. However, as we have significantly fewer stationary controller nodes we used more minor nodes for connections. Minor nodes in our model have high computational and execution power. VNA makes any node minor node based on its onboard resources. These minor nodes can act as 5G network MIFI-HotSpots until we can use technology like 5G small cell networks and MIMO on vehicles. This approach enables the nodes to become dynamic and mobile 5G source points, which will increase the overall range of the 5G network. The incentive mechanism motivates the nodes to

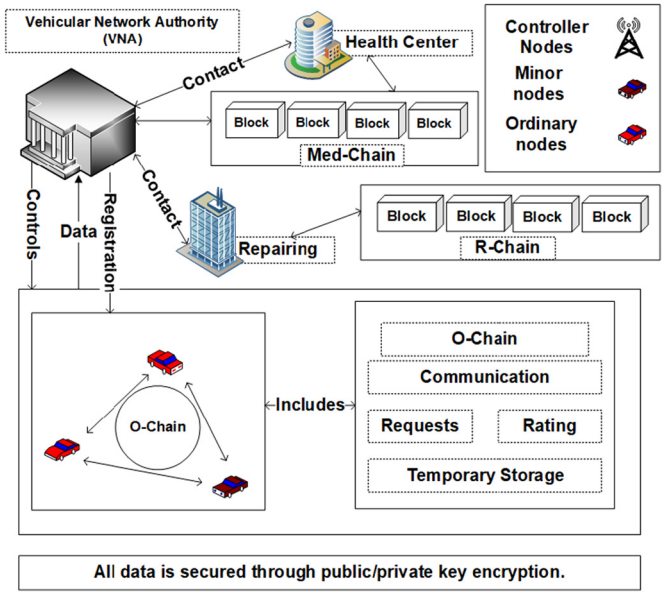

Fig. 12. Node Failure and Passenger Healthcare Management.

act as a minor node. The cost of 5G source point integration is handled 50% by VNA while the other 50% by the minor node owner which can be adjusted with given incentives. This approach helps to reduce the overall cost of the infrastructure and to increase the overall range of the 5G network. Using already present infrastructure for 5G deployment is a promising technique to achieve cost-effectiveness in any scenario.

4.8. Proposed algorithm

5G network has a higher frequency than 4G and traditional networks. Hence, due to high frequency and shorter wavelength, it has a lower range. In different scenarios, 5G may have a different range values from 200 m to 1000 m. However, the reliable range value will always be 70% of the total range.

Unlike 4G, 5G needs a lot more costly infrastructure because of its high-frequency waves that can only travel to low ranges. As higher frequency waves have shorter wavelengths and more bandwidth, this means that 5G has a shorter range but it can carry much more data.

Algorithm 1: CASE 1: Priority Based Ordinary Node Communication.

Input: Service requested
Output: Service received
if *ControllerNode = Present* **then**
  OrdinaryNode connects ControllerNode;
else if *ControllerNode = Not Present && MinorNode = Present* **then**
  if *Range* $>$ 700 **then**
    OrdinaryNode connects MinorNode;
  else if *Range* $<$ 700 **then**
    Connect:

Algorithms 1 and 2 represent case 1 and case 2 for the proposed priority based communication approach for nodes.

For example:

In the current proposed algorithms, the range value is 1000 m. Hence, we used 700 m. 5G provides a signal range of average 1000 m in which the minimum range in literature is around 200 m and 1.7 km is the maximum range. Los provides more coverage than NLos as 5G waves are non-penetrable waves.

Algorithm 2: CASE 2: Priority Based Minor Node Communication.

Input: Service requested
Output: Service received
if *ControllerNode = Present* **then**
  MinorNode connects ControllerNode;
else if *ControllerNode = Not Present && MinorNode = Present* **then**
  if *Range* $>$ 700 **then**
    MinorNode connects MinorNode;
  else if *Range* $<$ 700 **then**
    Connect:

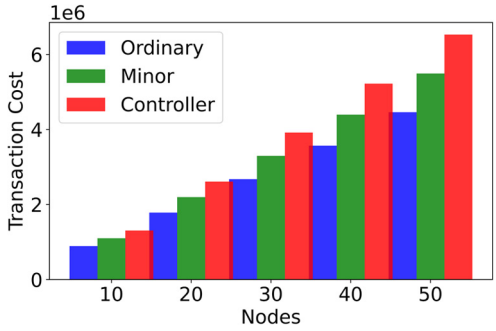

Fig. 13. Transaction Cost for Deployment of Nodes with respect to Scalability. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

5. Simulations and experimentation

Smart contracts of the proposed system are deployed on the operating system, Windows 10 Pro. The device used for simulation and experimentation has a core i5 processor of 7th generation, 8 GB Ram, and 4 GB shared graphics. The implementation is done using solidity language on tools including Remix and Ganache. Remix also provides fake accounts for experimentation and with each account provides 100 fake ether as balance. Ethereum platform is used which provides public blockchain with Proof of Work (PoW) consensus mechanism. Smart contracts are deployed and tested on the Remix to represent different tasks of vehicular networks. Metamask is used as a wallet. Sumo and Omnet++ are used with veins and inet modules to simulate a demo network to check the effectiveness of the proposed priority based approach. Python and Google Colaboratory are used for graphical representations.

6. Results and discussion

Scalability is achieved without sacrificing cost-effectiveness. Cost-effectiveness is achieved at different phases in the proposed model, which include reducing the cost at the deployment of nodes and reduction of the total cost while increasing scalability. Moreover, scalability is shown with respect to increasing cost. Cost is shown in the form of transaction cost and execution cost. With the increasing development of blockchain platforms and new versions of solidity language, execution cost decreases. Transaction cost depends on the number of variables and features used, which may vary in different implementation scenarios. Total time is also decreased for a single transaction as the total number of nodes needed for a single transaction are decreased.

6.1. Scalability and cost-effectiveness

As scalability is increased we need more infrastructure for the networks. As this infrastructure is costly we are using three kinds of nodes in our proposed architecture. Figs. 13 and 14 clearly describe the deployment cost in terms of execution and transaction

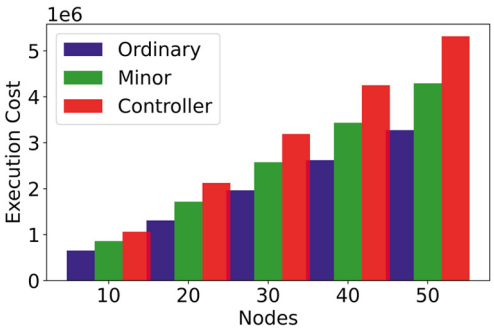

Fig. 14. Execution Cost for Deployment of Nodes with respect to Scalability.

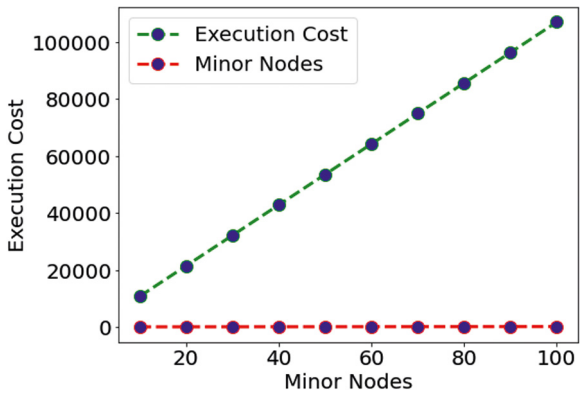

Fig. 15. Execution Cost of Minor Nodes with respect to Scalability.

cost for different nodes in the blockchain network with respect to scalability. With an increasing number of nodes, we can see the increasing cost for deployment. For deployment, the execution cost for a single controller node is 106305, for a single minor node, 85864, and for a single ordinary node is 65491. Transaction cost for a single controller node is 130521, for a single minor node, 109824, and for a single ordinary node is 89195. Transaction costs may vary with different features according to the implementation scenario. As Figs. 14 and 13 clearly show that the cost of controller nodes is much higher than minor nodes, while the cost of minor nodes is higher than ordinary nodes. Therefore in our proposed model we reduced the deployment of controller nodes to a minimum and used low-cost minor nodes and ordinary nodes. This reduction of controller nodes drastically reduces the deployment costs.

6.2. Minor nodes or forwarding nodes

Minor nodes or forwarding nodes are the main nodes after the controller nodes and the total cost of each transaction depends on the number of minor nodes involved in the transaction. As each minor node has its own transaction and execution cost. As the scalability increases more and more minor nodes are involved in the transaction thus increasing the total cost. In huge networks, this will cause costly transactions. Figs. 15 and 16 show the increase of transaction and execution cost with respect to scalability. As the number of nodes is increasing for a single transaction, the total cost also increases.

6.3. Time

The number of nodes plays an important role in any transaction and when scalability is achieved, more nodes are involved in transactions. Hence the total time of any transaction is directly proportional to the number of nodes used. Fig. 19 shows how time

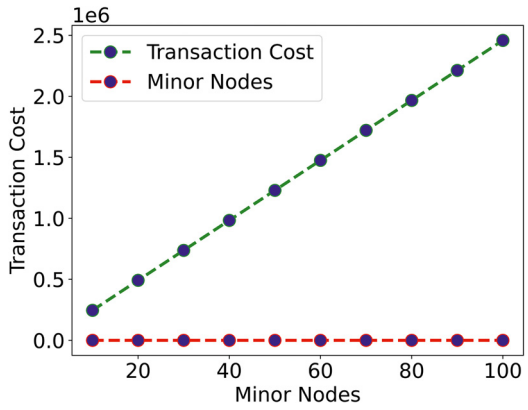

Fig. 16. Transaction Cost of Minor Nodes with respect to Scalability.

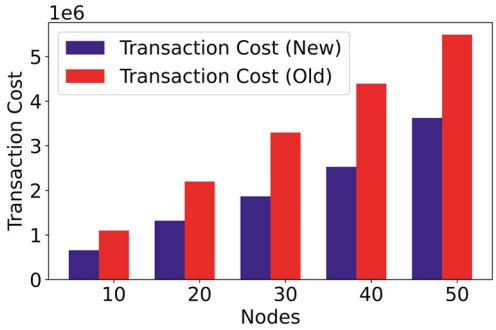

Fig. 17. Decrease in Transaction Cost with respect to Nodes.

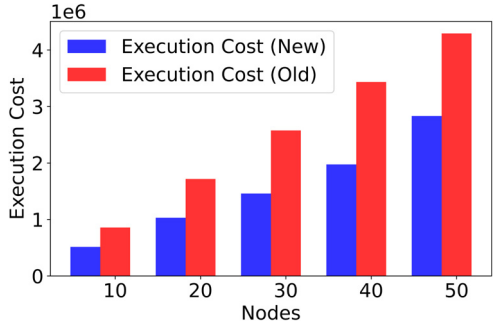

Fig. 18. Decrease in Execution Cost with respect to Nodes.

is increasing for a single transaction with an increasing number of nodes. If a single transaction takes, 1 sec for a single transaction between two nodes, 10 nodes will take 9 sec for a single transaction.

Fig. 20 shows how time is decreased by decreasing the number of nodes in each transaction.

6.4. Time and cost-effectiveness due to priority based techniques

As the number of nodes in a single transaction increase, the total time and cost also increases. Proposed priority based approach promises less number of nodes involved in each transaction, thus decreasing the, Time, total execution cost and transaction cost for each transaction. The graphical representation shows the difference between cost and time, before and after the use of the proposed approach. The decrease in the number of nodes after the proposed priority based approach is directly responsible for the decrease in overall costs and time which is shown by Figs. 17 and 18.

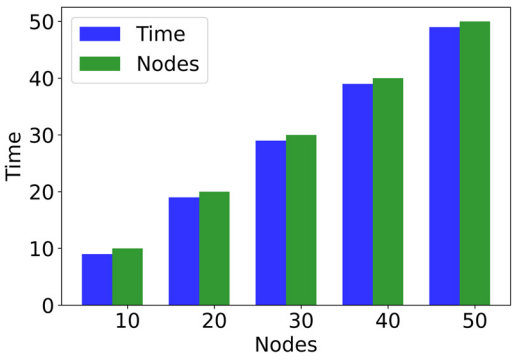

Fig. 19. Time Required for Transaction with respect to Nodes.

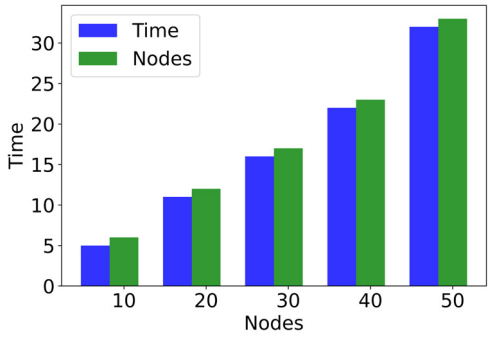

Fig. 20. New Time for Transaction with respect to New Number of Nodes.

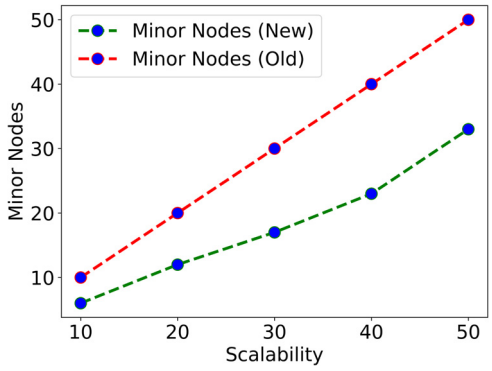

Fig. 21. Comparison of Minor Nodes after Priority based Approach with respect to Scalability.

6.5. Comparison between old and new nodes

For different scenarios, number of nodes may vary however in each case total number of nodes involved in the transaction decrease. To get an accurate number of nodes in the simulation we repeated the simulation and took the average number of nodes required for a complete transaction with respect to scalability. Due to this decrease in the total number of nodes in each transaction, the whole proposed model becomes scalable and cost-effective at the same time.

Fig. 21 shows the comparison of the number of minor nodes involved in each complete transaction before and after the proposed priority based approach. This decrease in total time affects the total cost and makes each transaction less costly, unlike the old model where cost was increasing with scalability. This provides us with a cost-effective model that can be scalable by increasing the number of nodes. The proposed priority based approach promises less number of nodes involved in each transaction, thus decreasing the time, total execution cost, and transaction cost for each transaction.

7. Conclusion

A comprehensive blockchain based vehicular network architecture is proposed in this research work. Our proposed architecture consists of different components, which are essential for a blockchain based vehicular network architecture. Each component in the proposed model is there to solve a particular problem keeping in mind the adaptability, cost-effectiveness, and scalability. The proposed model handles issues like scalability, high execution and transaction cost, adaptability, robustness, security, and privacy. We included an incentive mechanism in our proposed model to handle the selfishness of nodes and a reputation system to handle the maliciousness of nodes. Instead of using the same costly controller nodes, we used three different types of nodes, thus decreasing the total deployment cost, and using priority access techniques we made sure that fewer nodes are used for each transaction thus decreasing the total transaction time, execution, and transaction cost. Two different blockchains, O-Chain and C-Chain, are used to ensure privacy and security. VNA is used to control the whole vehicular network and it is assumed that VNA cannot be compromised in any way. Node failure and passengers' healthcare scenarios are also discussed in detail. 5G implementation scenario is also discussed for blockchain based vehicular network architecture with a robust and cost-effective approach.

Graphical representations clearly describe the increasing deployment cost, execution cost, transaction cost, and time with an increasing number of nodes and the deployment cost differences between different types of nodes. Simulations results clearly depict the effectiveness of the proposed architecture in terms of scalability, time, and cost-effectiveness. We concluded that the proposed architecture effectively handles different issues of blockchain based vehicular networks. With the execution cost of a single controller node as 106305, minor node as 85864, ordinary node as 65491, and transaction cost of a single controller node as 130521, minor node as 109824, ordinary node 89195 gas values respectively the total execution and transaction cost is decreased making the model cost-effective. Due to the distributed nature of blockchain technology, VNA handles the incentive mechanism and various tasks, thus, ensuring cost-effectiveness. Use of existing infrastructure, a priority based approach and decrease in all kinds of costs at each level of the proposed model a high level of cost-effectiveness is ensured.

8. Future work

In the future, we will handle the 5G deployment issues in a vehicular network architecture related to handoff, interference, and coverage in detail. It is assumed that VNA can not be compromised hence we will discuss different scenarios related to VNA in detail. The use of already present infrastructures in vehicular network architectures promises a cost-effective solution both for 5G technology and vehicular network architectures in a smart city.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The authors wish to thank the anonymous reviewers for their valuable suggestions.

References

[1] H. Kumar, M.K. Singh, M.P. Gupta, J. Madaan, Moving towards smart cities: solutions that lead to the Smart City Transformation Framework, Technol. Forecast. Soc. Change 153 (Apr. 2020) 119281, https://doi.org/10.1016/j.techfore.2018.04.024.

[2] K. Salah, M.H.U. Rehman, N. Nizamuddin, A. Al-Fuqaha, Blockchain for AI: review and open research challenges, IEEE Access 7 (2019) 10127–10149, https://doi.org/10.1109/ACCESS.2018.2890507.

[3] B. Fleming, Smarter and safer vehicles [Automotive Electronics], IEEE Veh. Technol. Mag. 7 (2) (2012) 4–9, https://doi.org/10.1109/MVT.2012.2190223.

[4] H. Mousannif, I. Khalil, S. Olariu, Cooperation as a service in VANET: implementation and simulation results, Mob. Inf. Syst. 8 (2) (2012) 153–172, https://doi.org/10.1155/2012/853853.

[5] K. Zhang, J. Ni, K. Yang, X. Liang, J. Ren, X.S. Shen, Security and privacy in smart city applications: challenges and solutions, IEEE Commun. Mag. 55 (1) (Jan. 2017) 122–129, https://doi.org/10.1109/MCOM.2017.1600267CM.

[6] H. Khelifi, S. Luo, B. Nour, H. Moungla, S. Hassan Ahmed, Reputation-based blockchain for secure NDN caching in vehicular networks, https://doi.org/10.1109/CSCN.2018.8581849, Dec. 2018.

[7] H. Khelifi, S. Luo, B. Nour, H. Moungla, S.H. Ahmed, M. Guizani, A blockchain-based architecture for secure vehicular Named Data Networks, Comput. Electr. Eng. 86 (Sep. 2020) 106715, https://doi.org/10.1016/j.compeleceng.2020.106715.

[8] T. Roosta, M. Meingast, S. Sastry, Distributed reputation system for tracking applications in sensor networks, https://doi.org/10.1109/MOBIQW.2006.361781, 2006.

[9] X. Huang, R. Yu, J. Kang, Y. Zhang, Distributed reputation management for secure and efficient vehicular edge computing and networks, IEEE Access 5 (Nov. 2017) 25408–25420, https://doi.org/10.1109/ACCESS.2017.2769878.

[10] M. Singh, S. Kim, Intelligent vehicle-trust point: reward based intelligent vehicle communication using blockchain, http://arxiv.org/abs/1707.07442. (Accessed 18 October 2020), Jul. 2017.

[11] Y. Xu, G. Wang, J. Yang, J. Ren, Y. Zhang, C. Zhang, Towards secure network computing services for lightweight clients using blockchain, Wirel. Commun. Mob. Comput. 2018 (2018), https://doi.org/10.1155/2018/2051693.

[12] K. Kaur, S. Garg, G. Kaddoum, F. Gagnon, S.H. Ahmed, Blockchain-based lightweight authentication mechanism for vehicular fog infrastructure, https://doi.org/10.1109/ICCW.2019.8757184, May 2019.

[13] D. Lin, Y. Tang, Blockchain consensus based user access strategies in D2D networks for data-intensive applications, IEEE Access 6 (2018) 72683–72690, https://doi.org/10.1109/ACCESS.2018.2881953.

[14] F. Grijpink, T. Härlin, H. Lung, A. Ménard, Cutting through the 5G hype: survey shows telcos' nuanced views, https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/Cutting-through-the-5G-hype-Survey-shows-telcos-nuanced-views. (Accessed 18 October 2020), 2019.

[15] B. Mafakheri, T. Subramanya, L. Goratti, R. Riggio, Blockchain-based infrastructure sharing in 5G small cell networks, in: 14th International Conference on Network and Service Management, CNSM 2018 and Workshops, 1st International Workshop on High-Precision Networks Operations and Control, HiPNet 2018 and 1st Workshop on Segment Routing and Service Function Chaining, SR+SFC 2018, 2018, pp. 313–317.

[16] I. Khan, M. Singh, D. Singh, Compressive sensing-based sparsity adaptive channel estimation for 5G massive MIMO systems, Appl. Sci. 8 (5) (May 2018) 754, https://doi.org/10.3390/app8050754.

[17] J. Zhang, X. Ge, Q. Li, M. Guizani, Y. Zhang, 5G millimeter-wave antenna array: design and challenges, IEEE Wirel. Commun. 24 (2) (Apr. 2017) 106–112, https://doi.org/10.1109/MWC.2016.1400374RP.

[18] W. Roh, et al., Millimeter-wave beamforming as an enabling technology for 5G cellular communications: theoretical feasibility and prototype results, IEEE Commun. Mag. 52 (2) (2014) 106–113, https://doi.org/10.1109/MCOM.2014.6736750.

[19] Y. Zhong, X. Ge, H.H. Yang, T. Han, Q. Li, Traffic matching in 5G ultra-dense networks, IEEE Commun. Mag. 56 (8) (Aug. 2018) 100–105, https://doi.org/10.1109/MCOM.2018.1700956.

[20] J. Chen, X. Ge, Q. Ni, Coverage and handoff analysis of 5G fractal small cell networks, IEEE Trans. Wirel. Commun. 18 (2) (Feb. 2019) 1263–1276, https://doi.org/10.1109/TWC.2018.2890662.

[21] M.A. Ouamri, M.E. Oteşteanu, A. Isar, M. Azni, Coverage, handoff and cost optimization for 5G heterogeneous network, Phys. Commun. 39 (Apr. 2020) 101037, https://doi.org/10.1016/j.phycom.2020.101037.

[22] F. Qamar, M.H.D.N. Hindia, K. Dimyati, K.A. Noordin, I.S. Amiri, Interference management issues for the future 5G network: a review, Telecommun. Syst. 71 (4) (2019) 627–643, https://doi.org/10.1007/s11235-019-00578-4.

[23] S.S. Sarma, R. Hazra, Interference mitigation methods for D2D communication in 5G network, in: Advances in Intelligent Systems and Computing, vol. 1040, 2020, pp. 521–530.

[24] J. Benseny, J. Walia, H. Hämmäinen, J. Salmelin, City strategies for a 5G small cell network on light poles, in: 2019 CTTE-FITCE: Smart Cities & Information and Communication Technology (CTTE-FITCE) https://doi.org/10.1109/CTTE-FITCE.2019.8894825.

[25] Y. Kryvenchuk, O. Vovk, A. Chushak-Holoborodko, V. Khavalko, R. Danel, Research of servers and protocols as means of accumulation, processing and

operational transmission of measured information, in: Advances in Intelligent Systems and Computing, Sep. 2020, pp. 920–934, 1080 AISC.
[26] S. Tuli, R. Mahmud, S. Tuli, R. Buyya, FogBus: a blockchain-based lightweight framework for edge and fog computing, J. Syst. Softw. 154 (Aug. 2019) 22–36, https://doi.org/10.1016/j.jss.2019.04.050.
[27] O. Novo, Scalable access management in IoT using blockchain: a performance evaluation, IEEE Int. Things J. 6 (3) (Jun. 2019) 4694–4701, https://doi.org/10.1109/JIOT.2018.2879679.
[28] Y. Ren, Y. Liu, S. Ji, A.K. Sangaiah, J. Wang, Incentive mechanism of data storage based on blockchain for wireless sensor networks, Mob. Inf. Syst. 2018 (2018), https://doi.org/10.1155/2018/6874158.
[29] B. Jia, T. Zhou, W. Li, Z. Liu, J. Zhang, A blockchain-based location privacy protection incentive mechanism in crowd sensing networks, Sensors 18 (11) (Nov. 2018) 3894, https://doi.org/10.3390/s18113894.
[30] M. Singh, S. Kim, Branch based blockchain technology in intelligent vehicle, Comput. Netw. 145 (Nov. 2018) 219–231, https://doi.org/10.1016/j.comnet.2018.08.016.
[31] Y.T. Yang, L. Der Chou, C.W. Tseng, F.H. Tseng, C.C. Liu, Blockchain-based traffic event validation and trust verification for VANETs, IEEE Access 7 (2019) 30868–30877, https://doi.org/10.1109/ACCESS.2019.2903202.
[32] Y. Zhang, J. Wen, The IoT electric business model: using blockchain technology for the Internet of things, Peer-to-Peer Netw. Appl. 10 (4) (Jul. 2017) 983–994, https://doi.org/10.1007/s12083-016-0456-1.
[33] Z. Zheng, et al., An overview on smart contracts: challenges, advances and platforms, Future Gener. Comput. Syst. 105 (Apr. 2020) 475–491, https://doi.org/10.1016/j.future.2019.12.019.
[34] W.J. Gordon, C. Catalini, Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability, Comput. Struct. Biotechnol. J. 16 (Jan. 2018) 224–230, https://doi.org/10.1016/j.csbj.2018.06.003.
[35] H. Kurdi, S. Alsalamah, A. Alatawi, S. Alfaraj, L. Altoaimy, S.H. Ahmed, Healthybroker: a trustworthy blockchain-based multi-cloud broker for patient-centered ehealth services, Electron. 8 (6) (May 2019) 602, https://doi.org/10.3390/electronics8060602.
[36] H. Zhong, Y. Geng, J. Cui, Y. Xu, L. Liu, A weight-based conditional privacy-preserving authentication scheme in software-defined vehicular network 9 (2020) 54, https://doi.org/10.1186/s13677-020-00198-3.
[37] C. Lai, R. Lu, D. Zheng, X.S. Shen, Security and privacy challenges in 5G-enabled vehicular networks, IEEE Netw. 34 (2) (Mar. 2020) 37–45, https://doi.org/10.1109/MNET.001.1900220.
[38] G. Kumar, et al., A privacy-preserving secure framework for electric vehicles in IoT using matching market and signcryption, IEEE Trans. Veh. Technol. 69 (7) (Jul. 2020) 7707–7722, https://doi.org/10.1109/TVT.2020.2989817.
[39] B. Mikavica, A. Kostić-Ljubisavljević, Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey, J. Supercomput., https://doi.org/10.1007/s11227-021-03659-x.
[40] X. Liu, H. Huang, F. Xiao, Z. Ma, A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs, IEEE Int. Things J. 7 (5) (May 2020) 4101–4112, https://doi.org/10.1109/JIOT.2019.2957421.
[41] M.N. Patwary, S. Junaid Nawaz, M.A. Rahman, S.K. Sharma, M.M. Rashid, S.J. Barnes, The potential short- and long-term disruptions and transformative impacts of 5G and beyond wireless networks: lessons learnt from the development of a 5G testbed environment, IEEE Access 8 (2020) 11352–11379, https://doi.org/10.1109/ACCESS.2020.2964673.
[42] M. Dai, S. Zhang, H. Wang, S. Jin, A low storage room requirement framework for distributed ledger in blockchain, IEEE Access 6 (Mar. 2018) 22970–22975, https://doi.org/10.1109/ACCESS.2018.2814624.
[43] K. Gu, N. Wu, B. Yin, W. Jia, Secure data query framework for cloud and fog computing, IEEE Trans. Netw. Serv. Manag. 17 (1) (Mar. 2020) 332–345, https://doi.org/10.1109/TNSM.2019.2941869.
[44] T. Jiang, H. Fang, H. Wang, Blockchain-based Internet of vehicles: distributed network architecture and performance analysis, IEEE Int. Things J. 6 (3) (Jun. 2019) 4640–4649, https://doi.org/10.1109/JIOT.2018.2874398.
[45] U. Arshad, S. Javaid, S. Ahmed, B. Seemab, N. Javaid, A futuristic blockchain based vehicular network architecture and trust management system, in: 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), pp. 1–6, https://doi.org/10.1109/aect47998.2020.9194160.
[46] P.K. Sharma, S.Y. Moon, J.H. Park, Block-VN: a distributed blockchain based vehicular network architecture in smart city, J. Inf. Process. Syst. 13 (1) (2017) 184–195, https://doi.org/10.3745/JIPS.03.0065.
[47] Z. Yang, K. Yang, L. Lei, K. Zheng, V.C.M. Leung, Blockchain-based decentralized trust management in vehicular networks, IEEE Int. Things J. 6 (2) (Apr. 2019) 1495–1505, https://doi.org/10.1109/JIOT.2018.2836144.
[48] M.A. Rahman, M.S. Hossain, M.M. Rashid, S. Barnes, E. Hassanain, IoEV-chain: a 5G-based secure inter-connected mobility framework for the Internet of electric vehicles, IEEE Netw. 34 (5) (Sep. 2020) 190–197, https://doi.org/10.1109/MNET.001.1900597.