Futuristic Decentralized Vehicular Network Architecture and Repairing Management System on Blockchain

Usama Arshad, Zahid Halim, Hisham Alasmary, and Muhammad Waqas, *Senior Member, IEEE*

***Abstract*—Blockchain technology is used often as a merger with other technologies to achieve a high level of security, privacy, and robustness and to handle issues, such as maliciousness of nodes, privacy leakage, the selfishness of nodes, communication delays, and high execution and transaction costs. There is currently a lack of a comprehensive system for automating and cost-effectively managing vehicle repairs, maintenance, and other associated services. To solve such issues, we proposed a novel futuristic comprehensive model that integrates a blockchain-based framework to safely record vehicle maintenance, validate repair services, and oversee parts inventory. It employs smart contracts and consensus protocols to secure communications and data storage, thus reducing data breaches and vulnerabilities from single-point failures. A reward system is embedded within the network to encourage positive behavior and deter detrimental actions. We also incorporated advanced privacy-ensuring methods, like zero-knowledge proofs and secure multiparty computation, to safeguard sensitive data while preserving its utility. Our model features automatic detection and response mechanisms for node failure, improving network resilience by 25% thus also providing a 20% reduction in execution, operational costs, and scalability with an enhancement of 15%, underscoring the model's efficiency in vehicular repair and maintenance activities. Results and simulations clearly depict the overall performance and efficiency in terms of security, privacy, node failure, and the management of vehicle repairs with respect to other closely related models.**

***Index Terms*—5G, blockchain, decentralized autonomous organization (DAO), incentive, intelligent transportation systems (ITS), repairing, vehicle network authority (VNA).**

I. Introduction

IN THE present era, vehicular network management solutions need to be effective as urban populations rise and the use of smart vehicles became more popular. With the potential to revolutionize several industries, and digital currencies, including finance, healthcare, supply chain management, and the Internet of Things (IoT), blockchain technology has emerged as a ground-breaking development [1]. Since there is no longer a need for central authorities or middlemen, participants can rely on the underlying technology to conduct transactions securely and transparently. An essential component of blockchain technology is support for smart contracts [2], self-executing agreements that autonomously enforce a contract's terms and conditions without requiring third parties to get involved. Decentralized finance (DeFi) [3], asset tokenization, supply chain management, and IoT applications are just a few of the many use cases that smart contracts make possible. Blockchain technology has become increasingly integrated into IoT systems in recent years, clearing the way for creative solutions to the problems with scalability, security, and data privacy that these systems face. IoT-based applications can boost trust, reliability, and resilience by utilizing the advantages of blockchain technology. A broad range of technology and applications are included in intelligent transportation systems (ITS), which are intended to increase the effectiveness, security, and sustainability of transportation networks [4]. The interchange of data on traffic conditions, road hazards, and other pertinent aspects is made possible by this vehicle-to-everything (V2X) connection [5], which enhances traffic management [6], lessens congestion, and boosts road safety. Global positioning systems (GPS), dedicated short-range communications (DSRCs) [7], and advanced driver-assistance systems (ADASs) are a few of the important technologies used in smart vehicle networks. Smart vehicular networks have a lot of potential, but they also have a lot of security, privacy, and trust issues to deal with. Traditional centralized network management strategies are frequently insufficient to protect the security and privacy of the enormous amounts of data generated by connected automobiles. By employing privacy-preserving methods like secure multiparty computation or zero-knowledge proofs (ZKPs) [8], blockchain-based ITS can also address the problems of privacy and trust in vehicle networks. These solutions make sure that private information is safeguarded while maintaining the advantages of blockchain technology, such as transparency and audibility. When compared to conventional methods, the vehicle-based secure blockchain consensus (VBSBC) algorithm [9] performs well in terms of authentication delay, key processing time, attack detection rate, throughput, and packet

Manuscript received 26 September 2023; revised 17 December 2023 and 20 March 2024; accepted 2 April 2024. Date of publication 9 April 2024; date of current version 26 June 2024. This work was supported in part by the Graduate Assistantship Scheme (GA-4) at Ghulam Ishaq Khan Institute of Engineering Sciences and Technology under Grant cs2201, and in part by King Khalid University through the Large Group Project under Grant RGP.2/373/45. *(Corresponding author: Usama Arshad.)*

Usama Arshad and Zahid Halim are with the Faculty of Computer Science and Engineering, Ghulam Ishaq Khan Institute, Topi 23460, Pakistan (e-mail: usamajanjua9@gmail.com; zahid.halim@giki.edu.pk).

Hisham Alasmary is with the Department of Computer Science, King Khalid University, Abha 62521, Saudi Arabia (e-mail: alasmary@kku.edu.sa).

Muhammad Waqas is with the School of Computing and Mathematical Sciences, Faculty of Engineering and Science, University of Greenwich, SE10 9LS London, U.K., and also with the School of Engineering, Edith Cowan University, Perth, WA 6027, Australia (e-mail: engr.waqas2079@gmail.com).

Digital Object Identifier 10.1109/JIOT.2024.3386600

loss rate. Smart contract-based incentive mechanisms can be used to assign benefits and penalties following predetermined standards, such as regular car maintenance, prompt vehicle repairs, and safe driving habits [10]. Encryption techniques help keep information secret during transactions, but they can make the system slower and harder to manage. Similarly, the rating system gives users a trust score based on their past actions to prevent bad behavior, but it is not perfect because new users might find it hard to prove they are trustworthy. However, this fosters transparency and trust by allowing all stakeholders to view and validate the reputation scores of other participants. For instance, customer reviews, successful completion of training or certification programs, and adherence to safety rules may have an impact on a mechanic's reputation score [11]. Another smart contract can handle the registration and reputation of mechanics and repair shops, keeping track of their performance, client feedback, and adherence to industry standards [12]. There is currently a lack of a complete system for automating and cost-effectively managing vehicle repairs, maintenance, and other associated services. This is a huge challenge for vehicle owners, repair shops, and other players in the automotive sector [13]. Furthermore, the lack of an efficient communication and information-sharing mechanism makes optimizing repair and maintenance arrangements difficult, resulting in higher costs and longer downtime for vehicle owners [14]. Moreover, the lack of a credible incentive structure and reputation management system can lead to issues such as self-interested nodes and a deficiency of trust among the parties involved, complicating the development and maintenance of effective collaborations [15], [16]. Potential vulnerabilities in centralized vehicular network authorities could lead to severe compromise. Such vulnerabilities, when coupled with the threat of node failures in a decentralized, blockchain-supported system, amplify these challenges [17]. Therefore, it becomes critical to formulate a strategy that leverages blockchain's scalability [18]. This plan should aim to provide a secure, economical, and automated solution for managing vehicular repairs and maintenance, along with related services [19]. Simultaneously, it should prioritize consistent communication and resource optimization to maintain an effective and efficient system. Fig. 1 clearly represents our recently proposed vehicular network architecture which handles different issues in terms of scalability, cost-effectiveness, and security [20]. However, like any model or technique, it had its own limitations. Our new proposed model handles different limitations in our recent work and also the gaps in the literature in terms of security, privacy, robustness, latency, and cost-effectiveness.

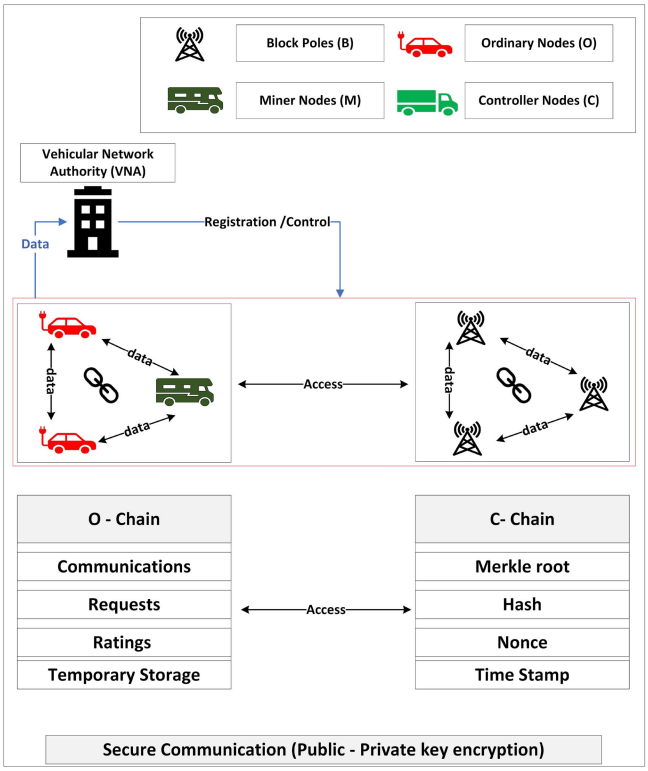

Fig. 1. Recent proposed vehicular network architecture.

A. Research Novelty and Contributions

1) We proposed a futuristic blockchain-based vehicular network architecture that integrates a novel car repair management system. This system is designed to log vehicle maintenance history, confirm repair services, and track component inventories, addressing key issues like scalability, security, robustness, and privacy.
2) By leveraging smart contracts and consensus algorithms, our architecture ensures secure data exchange within the network, enhancing both security and trust among participants.
3) We proposed a unique incentive mechanism and a reputation system to promote positive behavior within the network and deter malicious activities. This approach helps in maintaining a high-quality network environment.
4) The use of secure multiparty computation and ZKPs enables vehicle owners to share essential information without compromising their privacy, a critical aspect in today's interconnected world.
5) Autonomous node failure detection and response mechanism for vehicular networks is also included. This feature allows for immediate communication with the nearest repair facility in the event of a failure, significantly improving network resilience and safety.
6) The proposed solution demonstrates efficiency across various key performance indicators, such as authentication delay, processing time, execution time, execution cost, attack detection rate, throughput, and packet loss rate.

The research work is organized in the following manner. After the detailed introduction, in Section I, we have the main related work or the literature present in Section II with complete detail and a comparison of recent work. Section III contains some details about the technologies used in our work. Section IV describes in detail our proposed model. Section V briefly describes the implementation details and algorithms.

Section VI clearly depicts the results and their efficiency. Finally, Sections VII and VIII clearly describe our conclusions and what we may do in the future, respectively.

II. Related Work

Blockchain technology is flourishing and contributing to the latest innovation each day. A lot of work has been done on blockchain-based models in literature each having its limitations and possibilities. Zhang et al. [21] examined how mobility affects block propagation in VANETs while taking into account the special features that set these networks apart from conventional blockchain networks. Further study is required to examine the effects of this strategy on other blockchain structures, as this study primarily focuses on the single-chain structure in VANETs. Joshi et al. [22] provided a unique privacy-preserving data transmission architecture for cluster-based VANETs that makes use of blockchain technology. The Proof-of-Driving (PoD) technique is suggested by Kudva et al. [18] as a way to randomize the selection of honest miners for generating blocks effectively in blockchain-based VANET systems. With this strategy, existing consensus protocols like Proof of Work (PoW) and Proof of Stake (PoS) are addressed in terms of efficiency and fairness. Alladi et al. [23] undertook a thorough analysis of blockchain applications for protecting vehicular networks. They examined the role of cutting-edge developing technologies in blockchain-based vehicular networks and analyzed about 75 different blockchain-based security systems for vehicle networks. The authors offer helpful insights to steer further investigation into the topic by highlighting prevalent problems and potential research directions. Tandon et al. [24] reviewed blockchain-enabled vehicle networks and go over various blockchain-related vehicular network concepts. Although this article provides a thorough review, more research and practical applications are required to confirm the efficacy of different blockchain-based schemes in addressing the particular difficulties of vehicular networks. Mikavica and Kostić-Ljubisavljević [25] examined blockchain-based approaches for enhancing automotive network security services. They provide a useful resource for researchers and practitioners by giving concise comparisons of the various models that are accessible, highlighting their key attributes and goals concerning security, privacy protection, and trust management. Similarly, Han et al. [26] offered a thorough analysis of blockchain-related incentive mechanisms and how they complement one another. Devi and Pamila [27] presented a privacy-preserving blockchain-based incentive mechanism for an Android smartphone application that is based on an accident alert system. Although this approach seems promising, more testing and validation are needed to assess its effectiveness in the real world and any potential scalability problems. Litchfield and Khan [28] suggested BlockPres, a cutting-edge incentive system based on blockchain that aims to reduce disparities in prescription administration systems. By offering incentives for involvement, BlockPres hopes to motivate patients in underprivileged locations to interact with healthcare services. To stop fake news from spreading on social media platforms, Farooq et al. [29] described a decentralized framework that blends crowdsourcing and blockchain technology. The suggested method uses blockchain's immutable properties to hold people accountable and values them according to their reputation. Users receive rewards for good behavior and face consequences for bad behavior. Liu et al. [30] conducted an empirical analysis of the Steemit, a blockchain-based online community, user incentive mechanism. Using the social capital theory and psychological ownership theory as a framework, they investigate the effects of users' dual roles as social participants and community owners on their active participation behavior. Iqbal et al. [31] offered a safe fog computing method that keeps track of reputation ratings with the use of decentralized blockchain ledgers. In this strategy, fog vehicles are relieved of some of their duties by using roadside units (RSUs). In [32], we suggest a blockchain-based system for managing one's reputation in a P2P networking environment for the provision of bespoke manufacturing services. The authors provide a unique reputation evaluation approach to improve the precision and dependability of industrial production systems through the use of P2P networking and computing for Industrial IoT (IIoT) applications. Taking into account commercial projects and academic research, [33] provides a thorough evaluation and analysis of blockchain-based distributed trust and reputation management systems (DTRMS). The authors utilize a formal concept analysis to discover the widespread and consistent features of the research landscape, and they apply this study to the development of two taxonomies for blockchain and DTRMS. To reduce malicious routing in IoT networks, [34] proposes a blockchain-based reputation management system. This method overcomes the shortcomings of traditional RM systems for routers by leveraging blockchain as a distributed database for logging incident reports. The effectiveness and viability of the suggested method in detecting attacks and achieving system convergence were confirmed by simulation results. In [35], we see a reputation management system for automobile networks that are built on a hierarchical blockchain. The success of the reputation management system is greatly influenced by the suggested scheme, which aims to decrease block broadcast delay and increase blockchain throughput capacity. Because the blockchain is organized hierarchically, every car in the area has instantaneous access to every other car's most recent reputation value. Zhao et al. [36] suggested a blockchain-based mobile crowdsensing (MCS) reputation management system that is both dynamic and protects user privacy.

Rahman et al. [37] presented a secure Internet of Vehicles (IoV) architecture for controlling complex and ever-changing transport networks. In order to improve the effectiveness and transparency of ELV processing, [38] introduces ELVTrac, a complete framework. Integrating circular economy principles, blockchain technology, and distributed ledger technology, the framework uses smart contracts to coordinate the responsibilities of multiple stakeholders. We are moving toward the era of 6G, a future of dynamic and complex network structures that can only be handled using technologies, such as artificial intelligence (AI), the IoT, machine learning (ML), and blockchain. Data security is critical in a world where

TABLE I
RECENT PROPOSED MODELS IN LITERATURE WITH POSSIBLE LIMITATIONS

Ref No.	Proposed Model	Tools/Technology	Experimentation	Contributions	Limitations
[14]	Network traffic control and distribution system for vehicle networks based on learning to properly distribute communication and computation resources and boost the performance of next-generation wireless networks.	Core i7-9750H CPU and a GPU called the Nvidia GTX 1060 are used. TensorFlow and Python-3.6 were used for programming on a Linux system.	Four service providers, one mobile virtual network operator, four base stations, and four MEC servers made up the experiment configuration.	Formulation of a learning-based resource allocation strategy to raise the level of service in vehicle networks is the key contribution.	Limited in terms of real-world situations and the states of MEC servers. Additionally, security, privacy, and system robustness may not be clearly addressed in the paper.
[15]	A consortium blockchain-based reward system for ITS with a rating system and smart coins.	Blockchain and hashing techniques are used. (SHA256)	Fixed number of nodes are used and performance parameters include execution cost, transaction code, and delay.	A new cryptocurrency and incentive mechanism.	Limited due to the use of a fixed number of nodes and specific currency.
[16]	Automatic auto-insurance on blockchain to achieve decentralized nature.	Hyperledger Fabric as its foundation. The suggested concept uses Public Key Infrastructure (PKI), like a Certificate Authority (CA).	The three main transactions that are described in the paper are the processes for insurance transactions, accidents, and repairs.	Blockchain-based approach to speed up the handling of insurance claims and improve the trustworthiness and security of auto insurance contracts.	Limited in terms of implementation scenario and implementation details.
[17]	A vehicle-to-vehicle (V2V) blockchain-based energy trading scheme to improve security and efficiency using decentralized identifiers.	AVISPA simulation tool, blockchain technology, cryptography	The AVISPA simulation tool was used for security evaluations, and the approach was tested against man-in-the-middle and replay attacks.	Addresses the security flaws in present energy trading systems by proposing a blockchain-based energy trading system for V2V.	Limited in terms of scalability and implementation scenarios
[18]	Proof of Driving" (PoD) is proposed, an effective and scalable proof-variant with a filtering strategy based on the Service Standard Score (Sc) of car mining nodes for identifying and removing rogue nodes.	AVISPA simulation tool, blockchain technology, cryptography	The AVISPA simulation tool was used for security evaluations, and the approach was tested against man-in-the-middle and replay attacks.	Addresses the security flaws in present energy trading systems by proposing a blockchain-based energy trading system for V2V.	Limited in terms of scalability and implementation scenarios
[19]	Private Driver DNA proposed as a privacy-preserving approach	CARLA Tool is used. MPC is used.	They compared the ORE and HE strategies while protecting the drivers' privacy. The experiment made use of synthetic data generated by CARLA.	A unique architectural design. weighed the pros and cons of ORE and HE encryption methods in relation to ITS privacy-preserving solutions.	By extending the use of HE to compare ciphertexts, the infrastructure's potential may be expanded. Limited in terms of CARLA use.

TABLE II
CURRENT PROPOSED ARCHITECTURE VERSUS RELEVANT OLD MODELS

Paper Ref	**Security**	**Robustness**	**Reputation**	**Incentive Mechanism**	**Privacy**	**Repair / Maintenance**	**Scalability**	**Cost-effectiveness**
[14]		✓	✓					✓
[15]	✓		✓	✓	✓			
[16]	✓				✓		✓	
[17]	✓				✓			
[18]	✓				✓		✓	
[19]	✓	✓	✓					
Proposed Model	✓	✓	✓	✓	✓	✓	✓	✓

automobiles are interconnected with everything else around them. AI and ML have the ability to monitor a network continuously, like digital guards [39]. Now consider blockchain technology, which maintains data security and transparency. Although a little slow and power-hungry at times, it is part of this revolution. With ML, the blockchain process may be optimized to run more quickly and with reduced energy use. So, we may benefit from blockchain security without having to deal with its downsides [40]. As cars and other devices are constantly moving in these networks, it can be challenging to maintain a steady and quick connection. AI can be used to anticipate and control this ongoing mobility, ensuring that the network remains dependable and responsive even when it is moving. Spectrum management, also known as airwave management, is another interesting use of AI and ML. We anticipate using some extremely high-tech frequencies, such as terahertz waves, with 6G [41]. Introducing AI and ML to 6G networks is akin to giving these networks a super-brain, particularly in decentralized systems like those involving cars. This super-brain has the ability to intelligently handle futuristic

frequencies, maintain connections at high speeds, improve blockchain, and handle security [42]. Creating networks that are safer, smarter, and more powerful.

III. Preliminaries

A. Blockchain Technology

In its simplest form, blockchain can be demonstrated as a decentralized public leader. It regularly records transactions across several computers in a way that prohibits the recorded data from being retrospectively modified without also modifying all subsequent blocks, ensuring the durability and authenticity of the data [43]. The following are the main elements of a typical blockchain block:

1) block number/index;
2) nonce;
3) PoW consensus;
4) transaction list;
5) previous block hash;
6) Merkle root;
7) timestamp.

B. ITS Technology

The management and control of traffic have undergone a substantial improvement thanks to ITS. The name "ITS" refers to a wide range of applications, including traffic signal control systems, interchangeable message signs, automatic number plate identification, and collision avoidance systems. These systems gather real-time data from many sources, such as connected automobiles, roadside sensors, and traffic cameras, and then analyze it to produce helpful data [44]. In order to ease congestion and increase road capacity, for example, ITS can dynamically change the timing of traffic signals based on the volume of traffic at the time.

C. DAO

A decentralized autonomous organization (DAO) is an entity that operates on blockchain technology, devoid of centralized control. It is self-governing, transparent, and employs a democratic system wherein power is distributed among stakeholders who possess DAO tokens. These stakeholders have the power to propose, discuss, and vote on organizational decisions. The primary intent behind a DAO is to create an open, self-regulating system that operates without intermediaries [45]. DAOs are versatile and can be used for various purposes, such as collective financing, community decision making, and managing procedures in DeFi structures.

IV. Proposed Architecture

A. Overview

We proposed a futuristic blockchain-based vehicular network architecture and vehicle repair management system. With the potential to revolutionize the administration and upkeep of car networks, our model aims to handle critical concerns like scalability, security, privacy, and vehicle repair management in a way that is both innovative and realistic. The core of our proposed solution is a blockchain-based repair management system, which intends to provide a safe and open platform for logging vehicle maintenance history, validating repair services, and controlling part inventories in Fig. 2. The solution uses blockchain technology to deliver a high level of data integrity and traceability, making the records of repairs and components essentially tamper-resistant and simple to verify. In the field of auto repair and maintenance, this level of openness and confidence is unheard of.

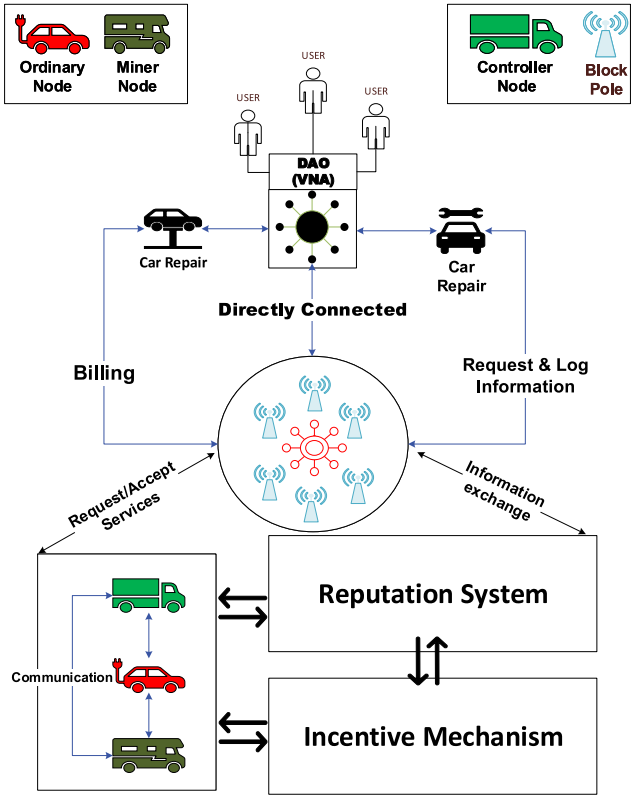

Fig. 2. Proposed blockchain-based vehicular network architecture.

B. Main Base Architecture

The proposed architecture has three main types of nodes based on their storage and computational complexities and RSUs which we termed as block poles:

1) ordinary nodes;
2) miner nodes;
3) controller nodes;
4) block poles.

Ordinary Nodes: The vehicles which have low computation power and low storage capability are the ordinary nodes. These nodes can not contribute much in terms of network stability and can ask for services from the controller nodes or other miner nodes.

Miner Nodes: Vehicles that have an average computation and execution power can contribute to the network. These nodes will act as relaying nodes too in the network and thus will help to make the overall network robust. These nodes will take part actively in the incentive mechanism and on-chain tasks.

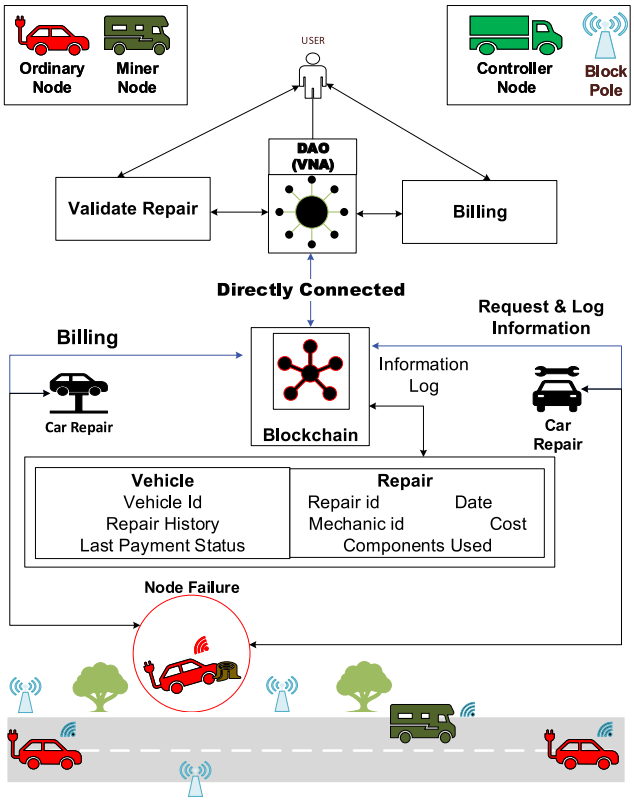

Fig. 3. Proposed blockchain-based repair management system.

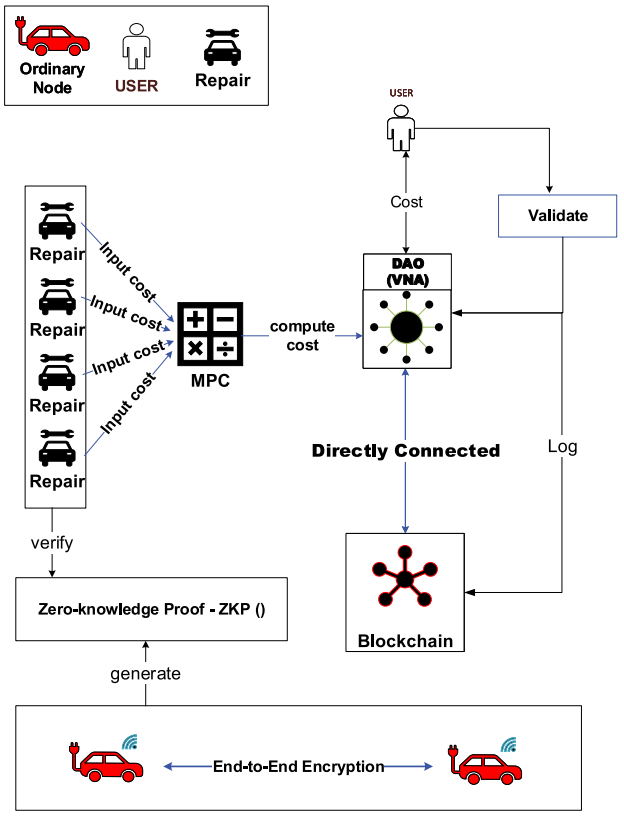

Fig. 4. Privacy and security (MPC, ZKP).

Controller Nodes: The vehicles which have the highest computational and execution power are fewer in number and they can handle the emergency tasks in case of any failures. These vehicles can play a vital role as miners and on-chain tasks. They can provide some services directly to ordinary or miner nodes when required.

Block Poles: The Block Poles are the RSUs in our architecture. They provide the services to the network when required. Block Poles keep a check on the network in terms of node failure and other services.

C. VNA as DAO

We replaced the vehicular network authority with a DAO, which represents a major departure from conventional approaches. The goal of this modification is to boost the system's democratic governance and autonomy. Apart from that the DAO also decreases the overall execution time of different processes.

D. Main Repairing Management Architecture

Our innovative blockchain-based repair management system is at the core of our proposed vehicular network architecture. This innovative, cutting-edge system has been designed to revolutionize vehicle repair and maintenance, making it a dependable, secure, and highly effective solution. Under the conventional system for vehicle repair, information regarding past restorations and maintenance can be disorganized, difficult to access, and susceptible to inaccuracy or tampering. This poses a significant problem for mechanics, who rely on this information to diagnose vehicle problems, and for vehicle owners who want to verify their vehicle's service history. Our approach addresses this issue by leveraging blockchain technology to provide a tamper-proof and completely transparent platform for documenting the maintenance history of vehicles. When a vehicle undergoes repair or maintenance, the date of repair, repair shop, mechanic, nature of the repair, components used, and cost are recorded in a blockchain-based ledger. This ledger is accessible by anyone, at any time based on permissions, and provides a complete, trustworthy record of every service performed on the vehicle. This precludes the possibility of fraudulent activities, such as altering the service history, overcharging, or performing unauthorized repairs. In addition, the system incorporates a validation mechanism for repairs. Each repair service performed on a vehicle is validated and verified to ensure that all repairs are valid and that all used materials are authentic. This not only guarantees the service's quality but also gives vehicle owners peace of mind. In addition, our system also manages inventory for repair services as illustrated in Fig. 3. By monitoring the use and availability of various vehicle parts, the system can notify repair services when certain parts are running low and must be reordered, ensuring they are always well stocked and ready to serve customers. In addition, if a node fails, our system automatically redirects the vehicle to the closest registered repair facility. The facility can then access the vehicle's repair history on the blockchain, enabling it to quickly and efficiently diagnose and resolve the issue. Billing can also be directly done on the blockchain thus decreasing the number of third parties and overall process time.

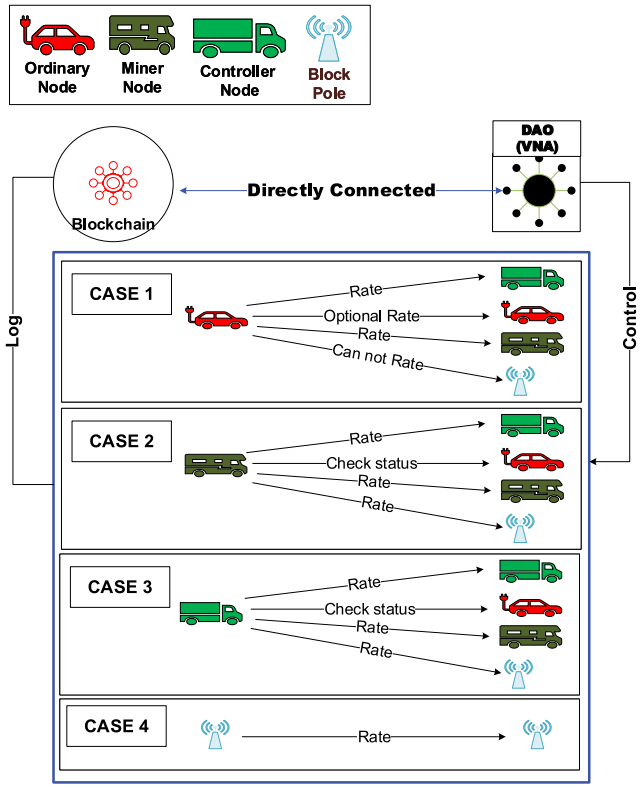

Fig. 5. Reputation system.

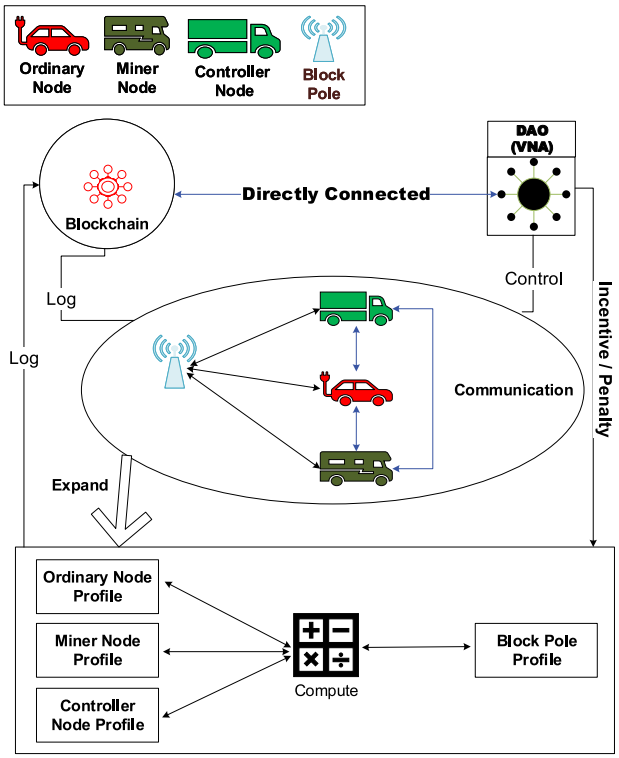

Fig. 6. Incentive mechanism.

E. Security and Privacy

Our system's emphasis on secure communication and data storage is a key component. We enable safe data interchange and storage inside the network by integrating smart contracts and consensus algorithms, significantly lowering the danger of data breaches and removing single points of failure, which are common in traditional centralized systems. In order to preserve private information while maintaining its usefulness, our approach incorporates cutting-edge methods like end-to-end encryption, secure multiparty computing (MPC), and ZKPs. As a result, nodes may exchange important information without risking an invasion of privacy. In our system, ZKP is used to conceal the identity of vehicles from repair shops. For a vehicle V and a repair shop R, a ZKP scenario is formulated as follows.

Let $P(V)$ be a predicate proving a statement about V. The ZKP allows V to validate $P(V)$ to R without revealing any details about V

$$\text{ZKP}_{V\to R}(P(V)). \tag{1}$$

This mechanism ensures that R receives only the necessary information for repairs without accessing private data about V. Similarly, MPC is used to achieve the reputation of each node without disclosing any information about the particular vehicle. All parties share their rating with the reputation system and then it is shared with an incentive mechanism that computes the penalty or incentive based on the individual reputation of nodes. Consider a scenario where multiple nodes $\{N_1, N_2, \ldots, N_k\}$ participate in an MPC protocol to compute a function f related to billing, without revealing their private inputs $x_1, x_2, \ldots, x_k$

$$\text{MPC}(f; x_1, x_2, \ldots, x_k) = y \tag{2}$$

where y is the computed output, ensuring that the individual inputs x_i remain confidential. However, using ZKP and MPC at the node level is not computationally effective. Hence, we used ZKP as illustrated in Fig. 4 to hide the identity of the vehicle from repair shops. This shows the repairing shops only necessary information without sharing private information about the vehicle. Hence, at the time of billing owners can validate the repair and pay without compromising any privacy.

F. Reputation System and Incentive Mechanism

Each node after communication with each other can provide a rating based on how good or bad the information provided was. The proposed reputation system as illustrated in Fig. 5 makes rating mandatory for the controller node and miner nodes as they contribute a lot to the network. Only Miner nodes and Controller nodes can rate the Block poles. Thus, this way the whole network is robust and node failures can easily be detected. Moreover, the selfishness of nodes or malicious nodes can also be detected based on their behavior in the network. Each Controller (C), Miner (M), and Block pole will have a rating profile on the blockchain based on which VNA can handle the nodes

$$R_{ij} = \begin{cases} R_{ij}^{(C)}, & \text{if node } i \text{ is a Controller node} \\ R_{ij}^{(M)}, & \text{if node } i \text{ is a Miner node} \end{cases} \tag{3}$$

where R_{ij} is the rating given by node i to node j. The rating scale is defined from 1 (lowest) to 5 (highest). The overall

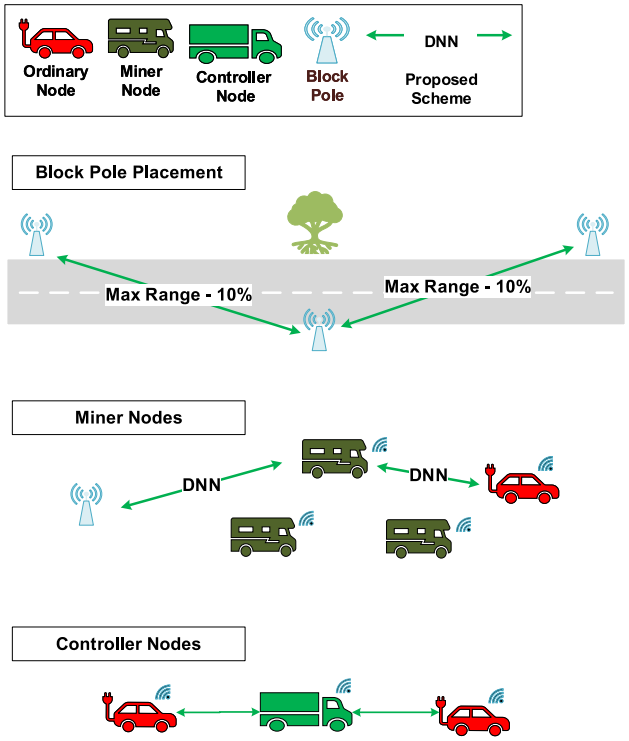

Fig. 7. Node deployment and communication strategy.

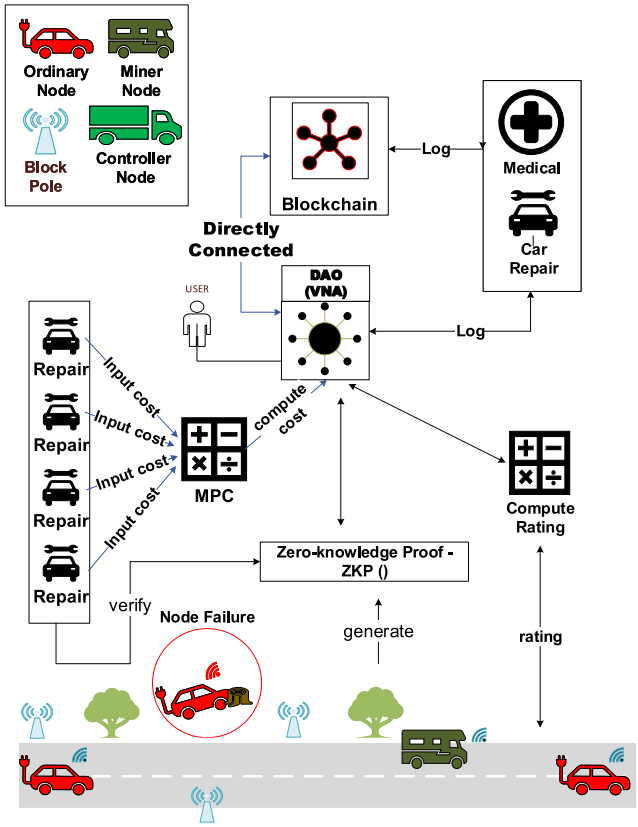

Fig. 8. Finalized proposed blockchain-based vehicular network architecture.

reputation score for a node j, denoted as Rep_j, is computed based on the accumulated ratings from other nodes

$$\text{Rep}_j = \frac{\sum_{i=1}^{N} R_{ij}}{N} \tag{4}$$

where N is the total number of ratings received by node j. As it aids in identifying node failures and detecting self-serving or malicious activity, this rating system is critical to preserving the integrity of the network. The vehicle network authority (VNA) can effectively administer and keep an eye on the nodes based on their reputation scores according to the ratings that are recorded on the blockchain. The unique incentive system in our proposed model as illustrated in Fig. 6 is intended to encourage positive network behavior and deter negative conduct. This system works by rewarding nodes for their beneficial contributions to the network and punishing them for their destructive behavior. This method fosters a network environment that is more dependable and secure. This also helps to eradicate the selfish behavior of nodes.

G. Node Failure

In addition, our model includes an autonomous node failure detection and reaction mechanism for the vehicular network. Controller nodes, Block poles, and Miner nodes check the status of the vehicles close by to find out if there is any kind of node failure. The onboard failures like sensor failures can be detected by the nodes themselves and reported while a complete failure can be detected by Block poles or miner nodes. The use of Controller nodes is optional in our network and they can be used depending on the requirement of the particular city or specific scenario. By enabling cars to immediately connect with the closest repair facility and transmit vital information like their position and service history after a failure, this feature improves network resilience and safety. In an emergency, the system may also divert traffic to the closest medical institution, improving safety and effectiveness.

H. Node Deployment and Communication Strategy

Network deployment and communication strategy play an important role to increase the overall efficiency of the proposed architecture in terms of scalability, cost-effectiveness, and robust communication as illustrated in Fig. 7. The deployment of current infrastructures like 5G is costly in real-world scenarios and hence this deployment needs an effective strategy more like a priority-based approach or need-based approach keeping in mind the challenges of current communication technologies like interference, low range, handoff, and nonpenetrateable waves. For our approach, greedy algorithms like Dijkstra can play a vital role in optimal and robust communication. Similarly, the placement of the block poles, the structure, and the number of nodes play a crucial role in cost-effectiveness and scalability as illustrated in Fig. 8. We proposed the placement of block poles based on the total range of the network and the need for the services in a specific area.

V. Implementation Details

For the implementation of the blockchain part, we used Remix and Solidity Language. Smart contracts are deployed

Algorithm 1 VNA Operations

S = system running state, N = total nodes, n = node, V = vote result
for each n **do**
  $R(n)$ = role based on computational power and resources
  $ID(n)$ = unique Node ID
  $B(n)$ = Store $ID(n)$, $R(n)$ and status on the blockchain
end for
Monitor and record node activities
if n underperforms or violates network rules **then**
  V = Initiate network vote for removing n
  if V = majority votes for removal **then**
    Update status of n on the blockchain
  end if
end if
for each n **do**
  Compute and update rewards/penalties and reputation score of n on the blockchain
end for

for each part of the proposed model on the Test Ethereum blockchain. To create and test the 5G vehicular network communication scenarios and traffic scenarios close to the real world, we used SUMO to generate traffic simulations, and NS3 was used to simulate networks for those traffic scenarios where required. The machine used for experimentation is Dell Precision 5820 Tower with 32-GB RAM and an Intel Xeon W-2275 processor. The operating system used is 64-bit Ubuntu 22.04. In order to confirm the efficacy and applicability of our proposed model, we carried out real-world testing scenarios. Several factors, mostly in terms of time, cost, scalability, and computation, including authentication delay, processing time, failure detection rate, throughput, execution costs, transaction costs, and packet loss rate, are used to evaluate the proposed solutions at each level of the proposed architecture. To clearly depict the implementation of the proposed model following are the proposed implemented algorithms.

A. Vehicle Network Authority Operations

Algorithm 1 manages node registration, network monitoring, and performance evaluation.

The blockchain network is connected to the VNA, which has been initialized, and node registration requests have been confirmed. Nodes are given roles based on their types, and their performance metrics are regularly evaluated. Nodes that consistently perform badly or violate the rules may be removed after a network vote. Node performance also has an impact on the rewards or penalties they receive, which are updated on the blockchain.

B. Vehicle Repair Management System

The management of vehicle repair is handled by Algorithm 2.

Algorithm 2 Vehicle Repair Management System

Require: V = Vehicle, R = Repair Node, D = Vehicle data, B = Repair bill, S = system running state, I = Repair Institute data, M = Mechanics, C = Components, H = Repair History, P = Payment status
for each active node n in S **do**
  if n is V and V breaks down **then**
    R = Assign closest Repair Institute using `minDistance`(Location(V), Location(I_i))
    D = `retrieveData`(V) from blockchain //including ID, repair history, last payment status
    M, C = `requiredRepair`(D)
    B = `computeBill`(M, C)
    `submitBillToVNA`(B, V, R)
  end if
end for
if payment_request from V is received **then**
  VNA prepares the final bill based on B, confirms with V and R
  P = `confirmPayment`(V, B)
  `updateBlockchain`(PaymentStatus(V) = P)
  H = `updateRepairHistory`(V, R, M, C)
  `updateBlockchain`(RepairHistory(V) = H)
end if

Algorithm 3 Privacy and Security

S = system running state, V = Vehicle, n = node, R = Repair Node, C = computed cost
for every interaction between V and R **do**
  Initiate encryption and ZKP protocol to maintain privacy
end for
if financial computations are needed **then**
  C = Use MultiParty Computation for optimal repair cost computation, maintaining individual cost privacy
end if
for every interaction between n and n' **do**
  n submits a rating for n'
  VNA/DAO verifies and updates the rating on the blockchain
end for

The system keeps track of the condition of each vehicle and notifies the closest Repair Institute to handle repairs when a failure happens. The blockchain is used to obtain the vehicle's data, including repair history and payment status. Following repair, the VNA examines the repair invoice, confirms payment, and updates the blockchain with the repair history and payment status.

C. Privacy and Security

Secure processing and communication are guaranteed by Algorithm 3. A ZKP protocol is started to verify information while retaining anonymity when sensitive data transfer is necessary.

Algorithm 4 DNN Algorithm

Require: O = Ordinary Nodes, M = Miner Nodes, C = Controller Nodes, B = Block Poles, N = All Nodes, R = Range, D = Density

Deploy N into network
for each n_i in O **do**
  if n_i requests service **then**
    Relay service via M
    if $D >$ threshold **then**
      Invoke C for service handling
    end if
    Fetch services from C or B as per availability and traffic condition
  end if
end for
for each connection $conn_i$ between nodes **do**
  if R_{conn_i} <= max_range * 0.9 and count($conn_i$) is minimum **then**
    Establish connection $conn_i$
  end if
end for

D. DNN Algorithm

Node deployment, communication, and traffic control are governed by Algorithm 4. The network's nodes are set up and registered on the blockchain. By obtaining services from Controller Nodes or Block Poles and relaying them to Ordinary Nodes, Miner Nodes serve as relay nodes. To manage the load during periods of high traffic, Controller Nodes are called. Connections are prioritized for nodes within this range with fewer connections based on a lower maximum signal range. On the blockchain, node status and network health are continuously analyzed and updated.

VI. Simulations and Results Discussion

A comparison of execution costs, gas values, and time in terms of delay, processing time, and computational costs is used to understand the efficiency of different phases of the proposed model.

A. Operations at VNA

The initial phase of our proposed approach includes the handling of different operations by DAO/VNA. VNA calculates the amount of penalty or incentive based on the performance of nodes. The graphical representation in Figs. 9 and 10 clearly describes the costs and time taken with respect to old models, respectively.

Using DAO as VNA handles robustness and scalability while maintaining the security and privacy of the system. In comparison to older models, most of these tasks are performed either manually or by some third party thus leading to the computational and execution time higher than automatic processes. Similarly using centralized platforms or manually handling processes leads to higher costs and breaches of security and privacy.

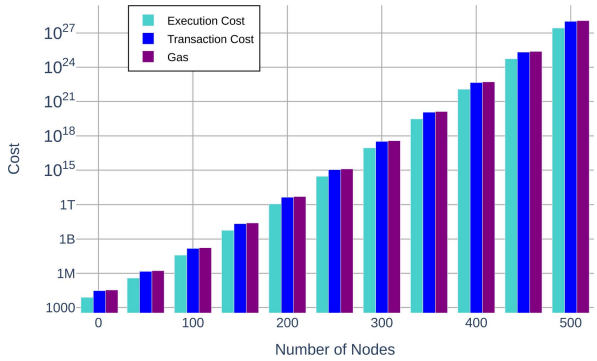

Fig. 9. Update nodes by DAO/VNA.

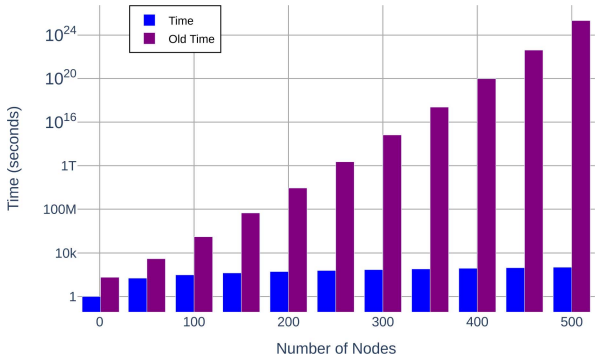

Fig. 10. Check node status by DAO/VNA.

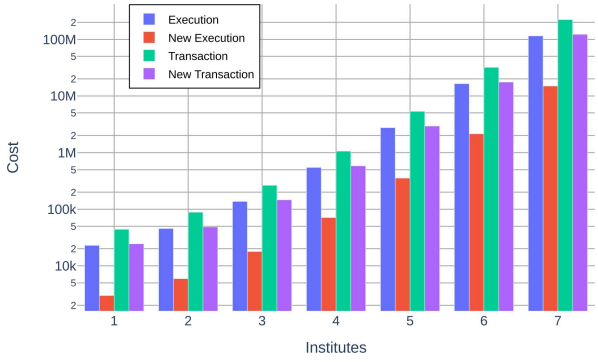

Fig. 11. Repair institutes versus total costs.

Hence, the graphical representations clearly show how our approach is far better in terms of time and cost when compared to any older technique or model.

B. Repairing Management

The placement of nodes, management of failures, and maintenance of nodes is the main goal of this proposed approach, however, graphical representations, in Figs. 11–13, clearly represent how our model performs better in terms of robustness, cost, and time. The load is shared by different institutes and as the number of node failures increases different institutes take care of them, depending on the availability and location.

Transaction and Execution costs show how any node coming a second time can benefit from almost half of the costs and time due to the logging of failures on the blockchain indicated

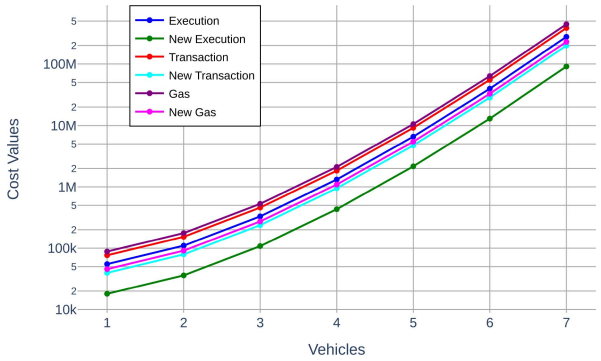

Fig. 12. Vehicles repaired versus cost.

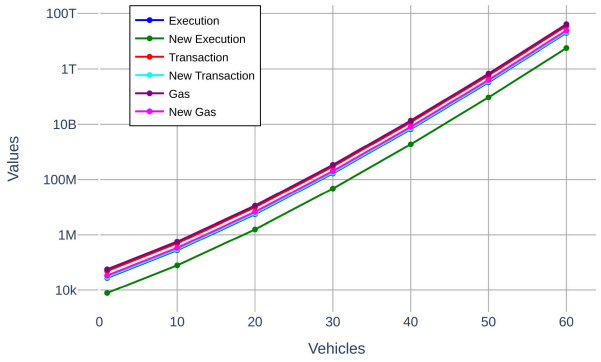

Fig. 13. Registered vehicles versus cost.

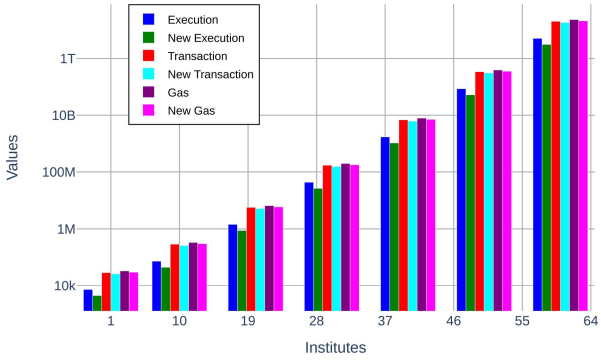

Fig. 14. Repair call versus cost.

by the Graphical representation in Fig. 14. First-time institutes register information on the chain which helps them quick maintenance in the future. Hence, when the number of vehicles is increased in an area or when the institutes have a load of work, that work is easily divided among them based on repair costs. Similarly, as the billing is online, this saves both time and overall costs. The increasing cost and time depict that when scalability is increased the overall cost, delay and processing time also increase.

C. ZKP Versus Cost and Time

To enhance the security and privacy of the overall model using ZKP and MPC helps to share information without sharing the actual data. However, as the graphical representation in Fig. 15 indicates that such techniques can be highly costly and time consuming when used in a scalable system. When

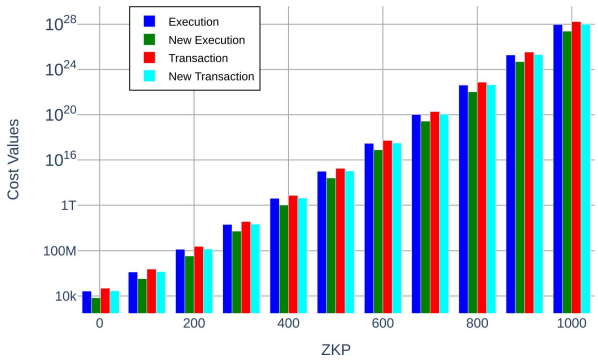

Fig. 15. ZKP versus cost.

the scalability increases the overall processing time, delay and costs also increase however due to the node placements and the overall structure of our proposed model and techniques the MPC or ZKP is only used for a small number of nodes thus decreasing the overall costs and processing time while maintaining security and privacy. Similarly, when it comes to using other greedy algorithms for node communication our proposed scheme provides the best results as we focused on less number of node communications at any specific time. Hence, similar to our old proposed techniques new techniques also enhance the overall network in terms of security, robustness, privacy, cost, delay, and processing times.

D. Comparative Analysis

The proposed model distinguishes itself by integrating robust security measures, a crucial aspect that previous models, notably [14], fall short in. Unlike [14] and [19], our model incorporates a unique incentive mechanism, encouraging positive behavior in the network, a feature shared only with [15]. Our approach to privacy, a paramount concern in current network systems, aligns with [15], [16], [17], and [18], but goes further in integrating this aspect with other advanced features. Additionally, the inclusion of repair and maintenance highlights our model's readiness for long-term sustainability, an aspect overlooked in other models. Using DAO and DNN removes a lot of manual processes and thus automatically reduces the execution and transaction costs as well as makes our model efficient in terms of time delays. We can calculate costs and time taken by different processes using the following mathematical equations.

Let T_{trad} represent the time consumed in traditional models. This includes data transmission, processing, and response time

$$T_{\text{trad}} = T_{\text{trans}} + T_{\text{proc}} + T_{\text{resp}} \tag{5}$$

where T_{trans} is the transmission time, T_{proc} is the processing time, and T_{resp} is the response time.

In the DAO model, let T_{DAO} represent the total time consumed, optimized through blockchain protocols and smart contracts

$$T_{\text{DAO}} = T_{\text{trans}} + T_{\text{proc, DAO}} + T_{\text{resp, DAO}}. \tag{6}$$

Here, $T_{\text{proc, DAO}}$ and $T_{\text{resp, DAO}}$ are optimized processing and response times in the DAO model.

The reduction in time consumption is given by

$$\Delta T = T_{\text{trad}} - T_{\text{DAO}}. \tag{7}$$

This equation represents the efficiency gain in the DAO model. The efficiency E in the DAO model can be quantified as

$$E = \frac{\Delta T}{T_{\text{trad}}} \times 100\%. \tag{8}$$

Our proposed model showcases a balanced, multifaceted approach, addressing key aspects like security, robustness, incentives, privacy, and scalability. It is an advanced and suitable choice for future wireless networks, demonstrating more time-efficient, responsive, and cost-effective qualities compared to traditional models.

VII. Conclusion

It is concluded that our proposed model provides a comprehensive futuristic model based on blockchain technology which solves different limitations of current architectures. Fundamentally, the main achievement of this study is the advancement of blockchain-based vehicle repair and maintenance management. By utilizing blockchain as a decentralized ledger for tracking all repair and maintenance activities, our proposed model tackles major problems head-on. This guarantees secure and verified record-keeping and makes it simple to obtain important data when needed. Additionally, the utilization of cutting-edge cryptographic techniques like MPC and ZKP safeguards network transactions and data, improving user privacy and security. To protect the secrecy and integrity of internal network traffic, end-to-end encryption was introduced. Our proposed architecture includes an incentive mechanism that encourages nodes to participate actively and constructively as a key component. On each part of the architecture, we made sure to keep in mind the cost-effectiveness and latency issues. Automation and on-chain tasks lead to faster processing, privacy, security, robustness, and traceability. The reputation system plays an important role in handling node failure detection and mitigation. The simulations and discussion section clearly depicts how our proposed model is efficient in terms of cost, time, scalability, and computation including authentication delay, processing time, attack and failure detection rate, throughput, execution costs, transaction costs, and packet loss rate. Our proposed model has the ability to significantly improve the security, efficiency, and overall performance of modern vehicle networks by providing a complete, secure, and efficient solution that fills in research gaps.

VIII. Future Work

In the future, we will work on the integration of AI technologies like object detection and digital twins in vehicular network architecture. Digital twins can mimic the whole vehicular networks, ITS, and using AI we can predict the future possible incidents forehand.

References

[1] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[2] Z. Zheng et al., "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020.

[3] J. R. Jensen, V. von Wachter, and O. Ross, "An introduction to decentralized finance (defi)," *Complex Syst. Inf. Model. Quart.*, vol. 30, no. 26, pp. 46–54, 2021.

[4] C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, and S. Jha, "B-FERL: Blockchain based framework for securing smart vehicles," *Inf. Process. Manag.*, vol. 58, no. 1, 2021, Art. no. 102426.

[5] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (V2X) testing," *Sensors*, vol. 19, no. 2, p. 334, 2019.

[6] J. Tang, A. McNabola, and B. Misstear, "The potential impacts of different traffic management strategies on air pollution and public health for a more sustainable city: A modelling case study from Dublin, Ireland," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. 102229.

[7] T. Petrov, L. Sevcik, P. Pocta, and M. Dado, "A performance benchmark for dedicated short-range communications and LTE-based cellular-V2X in the context of vehicle-to-infrastructure communication and urban scenarios," *Sensors*, vol. 21, no. 15, p. 5095, 2021.

[8] S. Sun, A. P. Petropulu, and H. V. Poor, "Mimo radar for advanced driver-assistance systems and autonomous driving: Advantages and challenges," *IEEE Signal Process. Mag.*, vol. 37, no. 4, pp. 98–117, Jul. 2020.

[9] T. Xie, J. Zhang, Y. Zhang, C. Papamanthou, and D. Song, "Libra: Succinct zero-knowledge proofs with optimal prover computation," in *Proc. Annu. Int. Cryptol. Conf.*, 2019, pp. 733–764.

[10] A. Ijjas, F. Pretorius, P. J. Steinhardt, and D. Garfinkle, "Dynamical attractors in contracting spacetimes dominated by kinetically coupled scalar fields," *J. Cosmol. Astropart. Phys.*, vol. 2021, no. 12, p. 30, 2021.

[11] Z. Noshad, A. Javaid, M. Zahid, I. Ali, R. J. U. H. Khan, and N. Javaid, "A blockchain based incentive mechanism for crowd sensing network," in *Proc. Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.*, 2020, pp. 568–578.

[12] M. Wang, Z. Zhou, and C. Ding, "Blockchain-based decentralized reputation management system for Internet of everything in 6G-enabled cybertwin architecture," *J. New Media*, vol. 3, no. 4, pp. 137–150, 2021.

[13] G. S. Kim and S. Goundar, "e-Governance and blockchain-based data supply chain for used cars," in *Distributed Computing to Blockchain*. Amsterdam, The Netherlands: Elsevier, 2023, pp. 377–387.

[14] M. Chen, T. Wang, K. Ota, M. Dong, M. Zhao, and A. Liu, "Intelligent resource allocation management for vehicles network: An A3C learning approach," *Comput. Commun.*, vol. 151, pp. 485–494, Feb. 2020.

[15] L. Vishwakarma and D. Das, "SmartCoin: A novel incentive mechanism for vehicles in intelligent transportation system based on consortium blockchain," *Veh. Commun.*, vol. 33, Jan. 2022, Art. no. 100429.

[16] A. S. Yadav, V. Charles, D. K. Pandey, S. Gupta, T. Gherman, and D. S. Kushwaha, "Blockchain-based secure privacy-preserving vehicle accident and insurance registration," *Expert Syst. Appl.*, vol. 230, Nov. 2023, Art. no. 120651.

[17] M. Kim, J. Lee, J. Oh, K. Park, Y. Park, and K. Park, "Blockchain based energy trading scheme for vehicle-to-vehicle using decentralized identifiers," *Appl. Energy*, vol. 322, Sep. 2022, Art. no. 119445.

[18] S. Kudva, S. Badsha, S. Sengupta, I. Khalil, and A. Zomaya, "Towards secure and practical consensus for blockchain based VANET," *Inf. Sci.*, vol. 545, pp. 170–187, Feb. 2021.

[19] G. Costantino, M. De Vincenzi, F. Martinelli, and I. Matteucci, "A privacy-preserving solution for intelligent transportation systems: Private driver DNA," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 1, pp. 258–273, Jan. 2022.

[20] U. Arshad, M. A. Shah, and N. Javaid, "Futuristic blockchain based scalable and cost-effective 5G vehicular network architecture," *Veh. Commun.*, vol. 31, Oct. 2021, Art. no. 100386.

[21] X. Zhang et al., "The block propagation in blockchain-based vehicular networks," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8001–8011, Jun. 2021.

[22] G. P. Joshi, E. Perumal, K. Shankar, U. Tariq, T. Ahmad, and A. Ibrahim, "Toward blockchain-enabled privacy-preserving data transmission in cluster-based vehicular networks," *Electronics*, vol. 9, no. 9, p. 1358, 2020.

[23] T. Alladi, V. Chamola, N. Sahu, V. Venkatesh, A. Goyal, and M. Guizani, "A comprehensive survey on the applications of blockchain for securing vehicular networks," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 1212–1239, 2nd Quart., 2022.
[24] R. Tandon, A. Verma, and P. Gupta, "Blockchain enabled vehicular networks: A review," in *Proc. 5th Int. Conf. Multimedia, Signal Process. Commun. Technol. (IMPACT)*, 2022, pp. 1–6.
[25] B. Mikavica and A. Kostić-Ljubisavljević, "Blockchain-based solutions for security, privacy, and trust management in vehicular networks: A survey," *J. Supercomput.*, vol. 77, no. 9, pp. 9520–9575, 2021.
[26] R. Han, Z. Yan, X. Liang, and L. T. Yang, "How can incentive mechanisms and blockchain benefit with each other? A survey," *ACM Comput. Surv.*, vol. 55, no. 7, pp. 1–38, 2022.
[27] G. S. P. Devi and J. M. J. Pamila, "Accident alert system application using a privacy-preserving blockchain-based incentive mechanism," in *Proc. 5th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, 2019, pp. 390–394.
[28] A. Litchfield and A. Khan, "Blockpres: A novel blockchain-based incentive mechanism to mitigate inequalities for prescription management system," *Sensors*, vol. 21, no. 15, p. 5035, 2021.
[29] M. Farooq, A. A. Makhdomi, and I. A. Gillani, "Crowd sourcing and blockchain-based incentive mechanism to combat fake news," *Combating Fake News with Computational Intelligence Techniques*. Cham, Switzerland: Springer, 2022, pp. 299–325.
[30] Z. Liu, Y. Li, Q. Min, and M. Chang, "User incentive mechanism in blockchain-based online community: An empirical study of steemit," *Inf. Manag.*, vol. 59, no. 7, 2022, Art. no. 103596.
[31] S. Iqbal, A. W. Malik, A. U. Rahman, and R. M. Noor, "Blockchain-based reputation management for task offloading in micro-level vehicular fog network," *IEEE Access*, vol. 8, pp. 52968–52980, 2020.
[32] Y. Lee, K. M. Lee, and S. H. Lee, "Blockchain-based reputation management for custom manufacturing service in the peer-to-peer networking environment," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 2, pp. 671–683, 2020.
[33] E. Bellini, Y. Iraqi, and E. Damiani, "Blockchain-based distributed trust and reputation management systems: A survey," *IEEE Access*, vol. 8, pp. 21127–21151, 2020.
[34] M. Li, H. Tang, and X. Wang, "Mitigating routing misbehavior using blockchain-based distributed reputation management system for IoT networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2019, pp. 1–6.
[35] W. Dong, Y. Li, R. Hou, X. Lv, H. Li, and B. Sun, "A blockchain-based hierarchical reputation management scheme in vehicular network," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6.
[36] K. Zhao, S. Tang, B. Zhao, and Y. Wu, "Dynamic and privacy-preserving reputation management for blockchain-based mobile crowdsensing," *IEEE Access*, vol. 7, pp. 74694–74710, 2019.
[37] M. A. Rahman, M. M. Rashid, S. J. Barnes, and S. M. Abdullah, "A blockchain-based secure internet of vehicles management framework," in *Proc. U.K./China Emerg. Technol. (UCET)*, 2019, pp. 1–4.
[38] R. Grati, F. Loukil, K. Boukadi, and M. Abed, "A blockchain-based framework for circular end-of-life vehicle processing," *Clust. Comput.*, vol. 27, pp. 1–14, Feb. 2023.
[39] J. Du, C. Jiang, J. Wang, Y. Ren, and M. Debbah, "Machine learning for 6G wireless networks: Carrying forward enhanced bandwidth, massive access, and ultrareliable/low-latency service," *IEEE Veh. Technol. Mag.*, vol. 15, no. 4, pp. 122–134, Dec. 2020.
[40] A. K. Tyagi, S. Aswathy, and A. Abraham, "Integrating blockchain technology and artificial intelligence: Synergies perspectives challenges and research directions," *J. Inf. Assur. Secur.*, vol. 15, no. 5, p. 1554, 2020.
[41] A. Kalla, C. De Alwis, P. Porambage, G. Gür, and M. Liyanage, "A survey on the use of blockchain for future 6G: Technical aspects, use cases, challenges and research directions," *J. Ind. Inf. Integr.*, vol. 30, Nov. 2022, Art. no. 100404.
[42] D. Unal, M. Hammoudeh, M. A. Khan, A. Abuarqoub, G. Epiphaniou, and R. Hamila, "Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things," *Comput. Secur.*, vol. 109, Oct. 2021, Art. no. 102393.
[43] A. S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustain. Energy Technol. Assess.*, vol. 52, Aug. 2022, Art. no. 102039.
[44] Q. Ren, K. L. Man, M. Li, B. Gao, and J. Ma, "Intelligent design and implementation of blockchain and Internet of Things–based traffic system," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 8, 2019, Art. no. 1550147719870653.
[45] L. Liu, S. Zhou, H. Huang, and Z. Zheng, "From technology to society: An overview of blockchain-based DAO," *IEEE Open J. Comput. Soc.*, vol. 2, pp. 204–215, 2021.

Usama Arshad received the B.S. degree in computer science from the University of Arid Agriculture, Rawalpindi, Pakistan, in 2018, the B.Ed. degree from Allama Iqbal Open University Islamabad, Islamabad, Pakistan, in 2020, and the M.S. degree in computer science from Comsats University Islamabad, Islamabad, in 2021. He is currently pursuing the Ph.D. degree in computer science with the Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Topi, Pakistan.

During master's and doctoral research, he worked in the domain of integration of blockchain and other emerging technologies (AI, ML, semantic Web, digital twins, and quantum) for better optimization in terms of scalability, cost-effectiveness, security, privacy, and robustness.

Zahid Halim received the B.S. degree in computer science from the Department of Computer Science, University of Peshawar, Peshawar, Pakistan, in 2004, and the M.S. degree in computer science and the Ph.D. degree from the National University of Computer and Emerging Sciences, Islamabad, Pakistan, in 2007 and 2010, respectively.

His Ph.D. degree was sponsored by the Foundation for Advancement of Science and Technology under the Faculty Development Program. During doctoral research, he worked in the domain of computational intelligence with the uncertain gaming environments as the test bed. Until 2012, he was the youngest indigenously produced Ph.D. in computer science by the country.

Hisham Alasmary received the M.Sc. degree in computer science from The George Washington University, Washington, DC, USA, in 2016, and the Ph.D. degree from the Department of Computer Science, University of Central Florida, Orlando, FL, USA, in 2020.

He is an Assistant Professor with King Khalid University, Abha, Saudi Arabia. His research interests include software security, IoT security and privacy, ML/DL applications in information security, and adversarial machine learning.

Muhammad Waqas (Senior Member, IEEE) received the Ph.D. degree from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2019.

From October 2019 to March 2022, he was a Research Associate with the Faculty of Information Technology, Beijing University of Technology, Beijing. Since April 2022, he has been an Assistant Professor with the Computer Engineering Department, College of Information Technology, University of Bahrain, Zallaq, Bahrain. He is currently a Senior Lecturer with the School of Computing and Mathematical Sciences, Faculty of Engineering and Science, University of Greenwich, London, U.K. He has also been an Adjunct Senior Lecturer with the School of Engineering, Edith Cowan University, Perth, WA, Australia, since November 2021. His current research interests are in the areas of wireless communications, vehicular networks, cybersecurity, and machine learning.

Dr. Waqas is an Associate Editor of the *International Journal of Computing and Digital Systems*. He is also a Guest Editor of *Applied Sciences* (MDPI). He is recognized as a Global Talent in the area of Wireless Communications by U.K. Research and Innovation.