Journal of
Sensor and Actuator Networks

MDPI

Article

Smart Automotive Diagnostic and Performance Analysis Using Blockchain Technology

Ahmed Mohsen Yassin [1,*,†], Heba Kamal Aslan [1,2,*,†] and Islam Tharwat Abdel Halim [1,2,*,†]

[1] School of Information Technology and Computer Science (ITCS), Nile University, Giza 12677, Egypt
[2] Center for Informatics Science (CIS), Nile University, 26th of July Corridor, Sheikh Zayed 12677, Egypt
* Correspondence: ahmed.yassin@valeo.com (A.M.Y.); haslan@nu.edu.eg (H.K.A.); ihalim@nu.edu.eg (I.T.A.H.)
† These authors contributed equally to this work.

Abstract: The automotive industry currently is seeking to increase remote connectivity to a vehicle, which creates a high demand to implement a secure way of connecting vehicles, as well as verifying and storing their data in a trusted way. Furthermore, much information must be leaked in order to correctly diagnose the vehicle and determine when or how to remotely update it. In this context, we propose a Blockchain-based, fully automated remote vehicle diagnosis system. The proposed system provides a secure and trusted way of storing and verifying vehicle data and analyzing their performance in different environments. Furthermore, we discuss many aspects of the benefits to different parties, such as the vehicle's owner and manufacturers. Furthermore, a performance evaluation via simulation was performed on the proposed system using MATLAB Simulink to simulate both the vehicles and Blockchain and give a prototype for the system's structure. In addition, OMNET++ was used to measure the expected system's storage and throughput given some fixed parameters, such as sending the periodicity and speed. The simulation results showed that the throughput, end-to-end delay, and power consumption increased as the number of vehicles increased. In general, Original Equipment Manufacturers (OEMs) can implement this system by taking into consideration either increasing the storage to add more vehicles or decreasing the sending frequency to allow more vehicles to join. By and large, the proposed system is fully dynamic, and its configuration can be adjusted to satisfy the OEM's needs since there are no specific constraints while implementing it.

Keywords: automotive; Blockchain; Diagnostic Trouble Codes (DTCs); vehicular communication

check for updates

Citation: Yassin, A.M.; Aslan, H.K.; Abdel Halim, I.T. Smart Automotive Diagnostic and Performance Analysis Using Blockchain Technology. *J. Sens. Actuator Netw.* **2023**, *12*, 32. https://doi.org/10.3390/jsan12020032

Academic Editor: Mingjun Xiao

Received: 7 February 2023
Revised: 6 March 2023
Accepted: 10 March 2023
Published: 7 April 2023

1. Introduction

The current structure of the automotive industry suffers from a lack of continuous monitoring regarding the information on the internal performance of the vehicles and the status of each internal part. This information is needed during the life cycle of vehicles from factory production until the first and second use. The lack of authentic information creates an untrusted problem regarding several issues including the history and performance of the vehicle, the originality of the changed parts, the lifetime of the changed parts, the recommended maintenance history, etc. This information along with the reliability of the vehicle's brand are the main factors that should be answered when buying a new car [1,2].

Commonly, Original Equipment Manufacturers (OEMs) do not track the real data about their vehicles after production. An example of the required data to monitor is the vehicle's performance in different environments such as the air conditioning performance in Africa and Europe. Hence, continuous and real-time vehicle monitoring could save much of the costs, as this leads to the early detection of defective parts. A well-known case of a lack of continuous monitoring is the case when TOYOTA discovered an issue with its airbags after producing thousands of vehicles. Due to the lack of continuous monitoring, this issue was not discovered, which cost the factory billions of USD. This could be discovered early by continuous monitoring, and fixing bugs could be performed using Flash Over The Air (FOTA) to upgrade or prevent such issues [3].

In addition, as autonomous driving is disrupting the automotive sector, continuous monitoring could gather information in the case of accidents to decide whether the responsibility for the accident is the software's or the manufacturer's [4]. Another aspect that could benefit from continuous monitoring is measuring the data concerning the amount of CO_2 emitted from the vehicles. Currently, this information is gathered by collecting samples in a specific area, which leads to a false indication. In addition, continuous monitoring could be used to collect information for vehicle forensics; however, solutions concerning vehicle forensics must maintain the driver's privacy. There are some solutions and trials, which are listed in the next section. All of them depend on collecting data manually [5,6] depending on human trust or a non-trusted system, which leads to untrusted results [7,8].

Besides, Blockchain technology is rapidly emerging as a disruptive force in the smart era, with a wide range of potential applications across multiple industries [9]. At its core, Blockchain is a decentralized, distributed ledger technology that enables secure, transparent, and tamper-resistant transactions and data sharing. It provides a platform for the creation of trustless environments where data can be securely and transparently shared and verified between parties, without the need for intermediaries. This technology has the potential to revolutionize various sectors, such as finance, supply chain management, healthcare, and many others, by enabling secure and transparent transactions and data sharing [10]. In recent years, Blockchain has gained attention in the field of the Internet of Things (IoT) and connected devices, where it can be used to enhance security and privacy, ensure data integrity, and enable new business models [11]. In particular, Blockchain has the potential to play a significant role in the development of the Internet of Vehicles (IoV), where it can provide a secure and reliable platform for data sharing and communication between vehicles, infrastructure, and other stakeholders [12].

Accordingly, in this paper, we propose a continuous monitoring system based on Blockchain technology. The proposed approach adopts Blockchain technology to address the challenges related to data trust and security in the automotive industry. The motivation behind this adoption lies in the fact that traditional data management systems, such as centralized databases, have limitations when it comes to ensuring data integrity, confidentiality, and authenticity. These limitations can lead to fraudulent activities, data tampering, and a lack of transparency, which can result in safety issues and decreased trust in the automotive industry. By using Blockchain technology, the proposed approach can provide a decentralized, transparent, and tamper-proof system that ensures the authenticity and integrity of the data stored in the network. Each block in the Blockchain contains a cryptographic hash of the previous block, which creates a chain of blocks that is resistant to modification. This makes it impossible to alter or delete the data without the consensus of the network participants, ensuring the immutability and integrity of the data. Furthermore, the use of encryption and symmetric cryptography in the proposed approach provides the confidentiality and authenticity of the data transferred from the vehicles to the OEM. This ensures that only authorized parties can access and modify the data, providing a secure and reliable system for collecting and analyzing the data. Overall, the adoption of Blockchain technology in the proposed approach aims to address the challenges related to data trust and security in the automotive industry, ensuring the safety and reliability of vehicles and increasing the trust of consumers in the industry.

The proposed system uses encryption to provide the following: confidentiality, integrity, and authenticity of data transferred from the vehicles to the OEM. Blockchain technology provides integrity for data saved in databases. Our system has the following advantages from an OEM's point of view: safety, branding, early detection of defective parts, and vehicle performance analysis. This is performed by sending periodic messages from the vehicle to its manufacturer's servers, which contain all the vehicle's logged Diagnostic Trouble Codes (DTCs), as well as a periodic check for the performance and originality of each part. On the other hand, the following advantages are from the owner's perspective:

safety, maintenance, and vehicle history. The vehicle's owner can check the vehicle's performance and the needed maintenance time. In addition, these data can be used as a proof of the vehicle's history in the case of resale, as data trust is provided using Blockchain, which prevents the modification of these data after they are published. Moreover, the manufacturer can use these data to analyze the performance of the vehicle in different environments. To create a system prototype, we used MATLAB Simulink to simulate both the vehicle and the Blockchain. In addition, OMNET++ was used to measure the expected system's storage and throughput.

Using Blockchain in our assumption covers some requirements in the system by increasing the trust and reliability of the extracted data. The decentralization feature gives more power to the system. In addition to transparency, immutability and access control are mandatory requirements to make the system secure and achieve the aim. The main contributions of this article are summarized as follows:

1. We propose a fully automated remote vehicle diagnosis system based on Blockchain technology that provides a secure and trusted way of storing and verifying vehicle data and analyzing their performance in different environments.
2. We investigated the benefits of the proposed system to different parties, such as vehicle owners and manufacturers, by providing reliable data on vehicle performance, history, and dependability. The system can also be adjusted to meet OEMs' needs without specific constraints during implementation.
3. We present several simulation results to evaluate the performance of the proposed system using MATLAB and OMNET++.

The remainder of this paper is organized as follows: Sections 2 and 3 depict the background on Blockchain and a literature review of the previous work. In Section 4, a detailed framework for our proposed system is discussed. In Section 5, the simulation of the proposed solution and a discussion of the results are given. Finally, the paper is concluded in Section 6.

2. Blockchain Background

2.1. Blockchain History

In 1991, Stuart Haber and Scott Stornetta introduced the idea of implementing a chain of blocks with cryptographic security to protect data against timestamp tampering. They named this chain "Bit gold", which was introduced, but never implemented. Bit gold was one of the earliest attempts at creating a decentralized virtual currency, proposed by Blockchain pioneer Nick Szabo in 1998. After two years, Stefan Konst published a unified theory of encryption protection chains, including some applications [13].

In 2008, Satoshi Nakamoto published his white paper, "Bitcoin: A Peer-to-Peer Electronic Cash System", in which he proposed a new form of digital currency; Bitcoin was implemented in 2009 [14]. The evolution of Blockchain started with Version 1.0 and continues to Version 2.0. While Version 1.0 is mainly concerned with Bitcoin and Cryptocurrency applications, Version 2.0 introduces financial applications such as smart contracts, Ethereum, and Hyperledger. The following consensus algorithms are used in Blockchain: Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Elapsed Time (PoET), Proof of Activity (PoA), Proof of Burn (PoB), and Proof of Capacity (PoC). For more information about these protocols, the reader can refer to [15,16].

2.2. Blockchain Overview

Blockchain is a way to store data in secure blocks on a trusted chain that cannot be modified. The block contains data, a hash, and the previous block hash, as shown in Figure 1. Because the blocks are arranged in a chain, any tampering with the block's data renders the chain invalid [17], as the hash will not match the next block, as shown in Figure 2. One of the main characteristics of the Blockchain is its distributed nature. Instead of using a central entity to manage the chain, Blockchain uses a peer-to-peer concept. Every new block is sent to be validated using one of the consensus algorithms stated earlier such as the PoW, in which the validators are called miners. The first miner who solves the mathematical puzzle will publish the block and receive rewards for his/her contribution. The puzzle is very complicated and needs high power and a huge amount of time to solve. For instance, in Bitcoin, it takes around ten minutes to validate and publish the block. To tamper with the Blockchain, the attacker needs to redo all the work performed in the PoW steps and take control of more than 50% of the peer-to-peer network, which makes this infeasible [18].

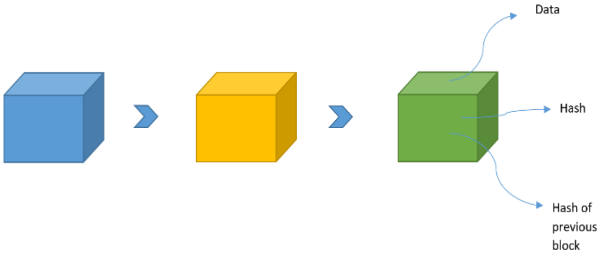


Figure 1. Blockchain architecture.

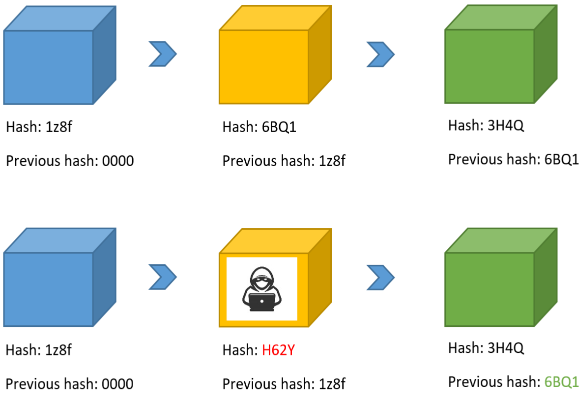


Figure 2. Blockchain before and after hacking.

Another widely used consensus protocol is the PoS, which aims to reduce the amount of computational work needed to verify the blocks and transactions. The PoS changes the way blocks are verified using the machines of coin owners. The owners offer their coins as collateral for the chance to validate blocks. Coin owners with staked coins become the "validators" and are selected randomly to "mine" or validate the block. This system randomizes who can "mine" rather than using a competition-based mechanism like the PoW. To become a validator, a coin owner must "stake" a specific number of coins. For example, Ethereum will require ETH 32 to stake before a user can become a validator. Table 1 shows a comparison between the PoW and PoS.

Table 1. Comparison between the PoS and PoW.

PoS	PoW
Block creators are called validators	Block creators are called miners
Energy efficient	Not energy efficient
Scalable	Not scalable
Network control can be bought	Robust security due to expensive upfront requirement
Validators receive transactions fees as rewards	Miners receive block rewards
Participants must buy coins or tokens to become a validator	Participants must buy equipment and energy to become a miner

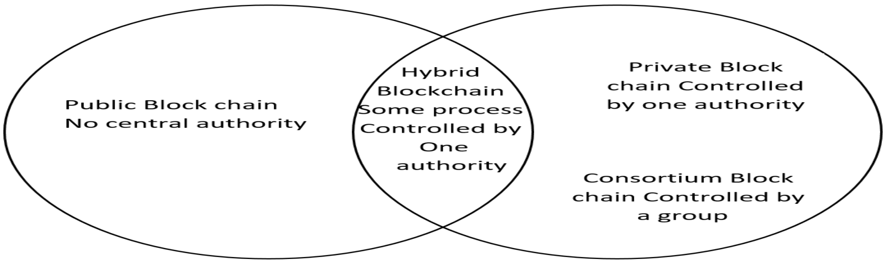


Figure 3. Types of Blockchains.

2.3. Types of Blockchains

Four types of Blockchains are commonly used, as follows: public Blockchain, private Blockchain, consortium Blockchain, and hybrid Blockchain. Figure 3 depicts the various types of Blockchains mentioned below [19,20]:

1. **A public Blockchain:** This is a permissionless network without any restrictions. Any node has the authority to be a part of the network and participate in it or record or verify transactions. In addition, it can perform the PoW. It has no centralized authority and is not regarded as a secure network.
2. **A private Blockchain:** This is a restricted network with permissions; thus, it is considered a closed network. The selected node has the authority to be a part of the network and participate in it or record or verify transactions. In addition, it can perform the PoW. One authority controls the network, so it can be considered a secured network.
3. **A consortium Blockchain:** This is a restricted network with permissions; thus, it is considered a closed network. More than one group has the authority to be a part of the network and participate in it or record or verify transactions. In addition, it can perform the PoW. A group controls the network, so it can be considered semi-centralized. Moreover, it is considered a secure network.
4. **A hybrid Blockchain:** This is a network with permissions for some parts and no permissions for others. Selected nodes have the authority to be a part of the network and participate in it or record or verify transactions. In addition, it can perform the PoW. One authority controls the network, and it can be considered a secured network with no permissions for some processes.

2.4. Characteristics of Blockchain

Blockchain has several unique characteristics compared to centralized databases. In what follows, the peerless characteristics of Blockchain are listed [21,22]:

- **Decentralization:** Blockchain is a distributed network without a central authority. This decentralization gives more power to the Blockchain, as there are many copies on different machines, which makes it very difficult to hack.
- **Transparency:** All the participants in the Blockchain have a copy of all transactions, and the stored data cannot be modified, which gives the Blockchain a high level of trust in the stored data. In addition, specific nodes, depending on the used algorithm, have to review each block.
- **Immutability:** This is measured by the ability of the Blockchain to stay secure without any tampering. Once a block is validated by cryptographic hashing and stored, it cannot be changed. This also increases trust and accuracy in the Blockchain.
- **Access control:** Depending on the Blockchain network used, users can have access to specific information or processes.
- **Consensus:** This is a voting process used to validate data from multiple sources before storing them in the Blockchain. It allows one to design a network using various consensus algorithms or distributed ledgers.
- **Anonymity:** Blockchain uses the user's address and a cryptographic algorithm to increase anonymity. In addition, the data sent are encrypted in a secure way.

3. Literature Review and Related Work

The Internet of Vehicles (IoV) is a rapidly growing technology that is transforming the transportation industry by enabling communication between vehicles and infrastructure, resulting in more efficient and safer roads. The IoV includes a wide range of applications such as traffic management, Vehicle-to-Vehicle (V2V) communication, Vehicle-to-Infrastructure (V2I) communication, autonomous driving, and smart transportation systems [23]. The recent advances in communication technologies such as 5G, edge computing, and Blockchain have accelerated the growth of the IoV by providing low-latency, high-bandwidth, and secure communication channels. The IoV has the potential to reduce traffic congestion, improve road safety, and enhance the overall driving experience for users. Therefore, the development of IoV applications and frameworks is crucial for the future of the transportation industry.

In this context, a Mobile-Edge-Computing (MEC)-based framework for the IoV is a crucial innovation that has emerged in recent years. The framework integrates the benefits of MEC and the IoV to enable efficient and reliable communication, data processing, and storage between vehicles, infrastructure, and the cloud [2]. In particular, the offloading method in 5G Heterogeneous Networks (HetNets) is one of the critical aspects of the MEC-based framework for the IoV. It enables the transmission of computationally intensive and data-intensive tasks from the vehicles to the MEC servers located at the edge of the network, which can significantly reduce communication latency and enhance the overall system performance. The offloading method in 5G HetNets is, therefore, crucial to realize the full potential of the IoV and enable various applications such as autonomous driving, real-time traffic monitoring, and intelligent transportation systems [24].

Hence, the IoV has revolutionized the automotive industry by enabling vehicles to communicate with each other and with the surrounding infrastructure. One of the key applications of the IoV is continuous monitoring and a remote diagnostic system for vehicles [25]. By integrating sensors and connectivity technologies, vehicles can generate a large amount of data related to their performance and health, which can be transmitted to the manufacturer's servers in real-time for analysis. These data can then be used to diagnose potential issues, identify defective parts, and perform proactive maintenance to avoid breakdowns. Furthermore, with the help of advanced analytics techniques, manufacturers can gain insights into the vehicle's behavior and performance, optimize their production processes, and enhance customer experience. The continuous monitoring and remote diagnostic system based on the IoV has the potential to reduce maintenance costs, improve vehicle safety, and enhance overall efficiency [26].

Besides, the emergence of connected vehicles and the IoV has brought about new challenges related to security, privacy, and trust in the automotive industry. In this context, Blockchain technology has been proposed as a promising solution due to its features such as decentralization, immutability, and transparency [27]. A Blockchain-based framework for the IoV can increase trust and traceability, prevent fraud and cyber-attacks, and ensure the confidentiality, integrity, and authenticity of the exchanged data. This can have significant implications for various aspects of the automotive industry, such as vehicle safety, maintenance, performance analysis, and vehicle history. Thus, a Blockchain-based framework for the IoV has the potential to revolutionize the automotive industry and enable new services and business models [28]. In the remainder of this section, we will provide an overview of similar systems and related work that have been proposed in the literature to address the challenges of continuous monitoring and remote diagnostic systems for vehicles in the context of the Internet of Vehicles.

As shown in Figure 4, the initial trial to collect the data for the purpose of continuous monitoring was accomplished by collecting DTCs using an On-Board Diagnostics (OBD) device and sending them to a server via WiFi [29]. The drawback of this system is that it does not use any means of encryption, which makes it insecure. In addition, the data should be collected at a certain time on one server, which represents a single point of failure.

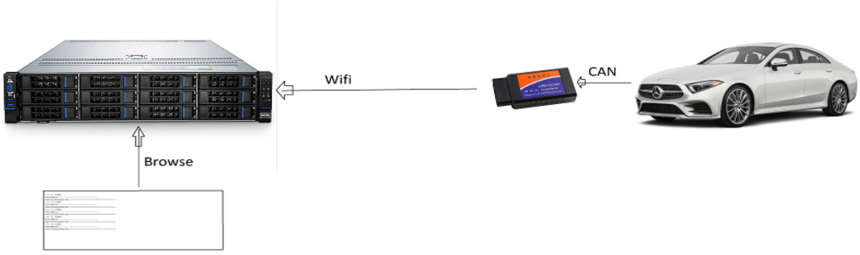


Figure 4. Collecting data using OBD device and WiFi [29].

An advanced trial was introduced using Blockchain technology, in which the Blockchain was used as a database for tracking vehicles' histories and service maintenance; the system was named "BCVehis" [30]. It allows all contributors, such as the vehicle's owner, maintenance workshop, dealer, insurance company, etc., to contribute with blocks for continuous monitoring of the vehicle's history and services. The system proposes to log every detail in the vehicle's life cycle manually to create a chain that contains the entire vehicle's history. The main disadvantage of this system is that the data must be collected and reviewed manually by the vehicle's insurance company. This system is illustrated in Figure 5.

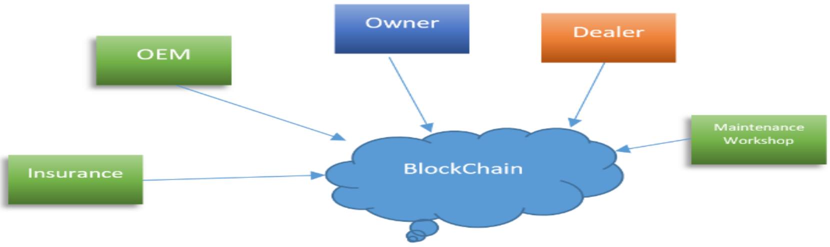


Figure 5. BCVehis [30].

Another proposal was presented in [31], in which the authors proposed a transaction management system for used car trading. The aim of this study was to create a smart contract based on a public Blockchain (Ethereum) without the need for a third party. The system depends on adding information manually from different participants and having it verified by trusted nodes. This leads to the possibility of being hacked or intentionally adding false information; therefore, the problem of trust persists. This system is depicted in Figure 6.

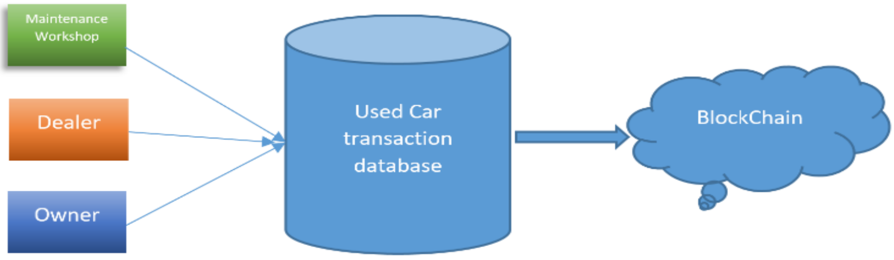


Figure 6. The Blockchain system in [31].

Another issue was raised due to the leakage of data, as discussed in [32]. It was shown how the recall process happens and how to report an issue to the OEM. The main issue with this process is that end users are highly involved in the detection and reporting processes, which leads to a lack of trust in this brand. The recall process is shown in Figure 7. Another trial proposed a Blockchain architecture for smart cities to collect data and upload it to the Blockchain [33]. Here, we face the same problem of manually collecting data, which jeopardizes the reliability of the collected data. Figure 8 depicts this system.

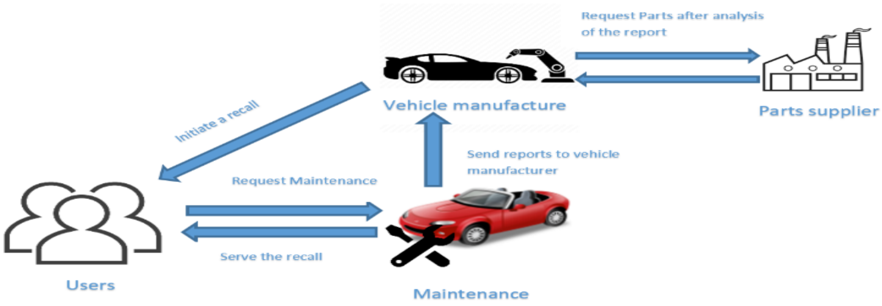


Figure 7. Recall process after manually reporting from the maintenance center.

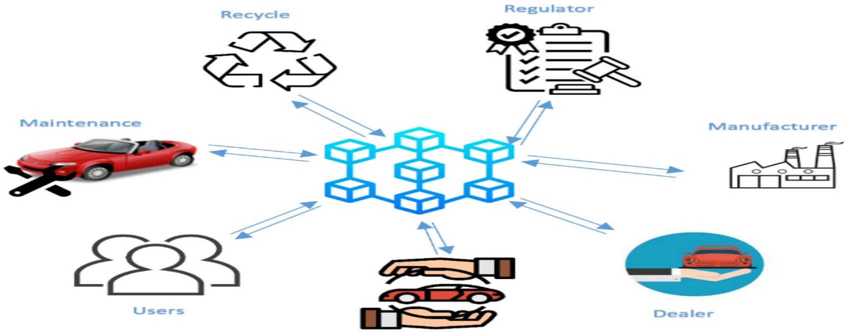


Figure 8. Blockchain distributed system in smart cities for automotive industry.

Existing systems in the field of vehicle diagnosis systems have several limitations that need to be addressed. One of the primary limitations is the lack of automatic data collection and verification mechanisms, which can lead to errors and inconsistencies in the stored data. Additionally, many similar systems are not embedded inside the vehicle itself, which can limit the accuracy and timeliness of the data collection process. Furthermore, authentication of the data sources and authorized access to the system are often not robust enough, which can result in unauthorized access and data breaches. Finally, the integrity of the data is not always ensured, which can be crucial in scenarios such as accident investigations. Table 2 provides a feature comparison of the existing systems.

Table 2. Feature comparison of existing systems.

Feature	[29]	[30]	[31]	[32]	[33]
Automatic collecting data	Yes	No	No	No	No
Embedded inside vehicle	Yes	No	No	No	No
Confidentiality	No	No	Yes	No	Yes
Authentication	No	No	Yes	Yes	Yes
Encryption	No	No	Yes	Yes	Yes
Integrity	No	No	Yes	Yes	Yes

4. The Proposed Blockchain-Based, Fully Automated Remote Vehicle Diagnosis System

4.1. Proposed Solution

As shown in Figure 9, the proposed solution consists of four layers, which are used to establish secure communication with the Blockchain. In the following paragraphs, we will describe each part of the system. We recommend using the consortium Blockchain type, as it is considered a private Blockchain with special access to specific groups, so each OEM can create a group with specific access and settings. In addition, we recommend using the PoW consensus mechanism, as it is the most-secure way to validate data. The OEM's server will be the miner responsible for mining and validating the data. This results in power consumption being transferred to the server side, while vehicle power consumption is minimized. The four layers of the proposed solution are given as follows:

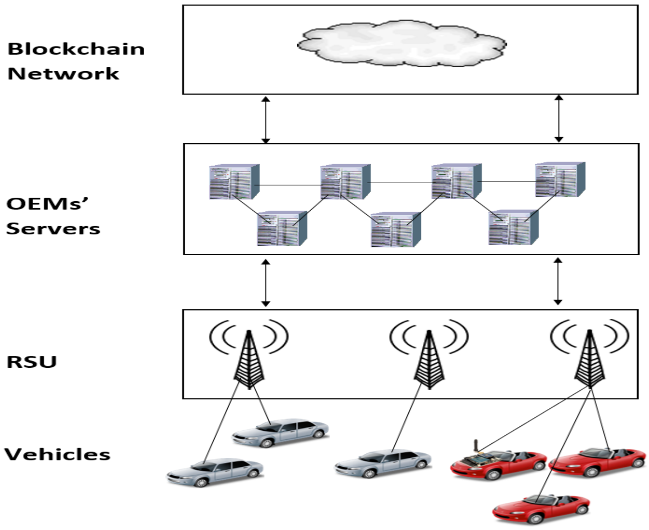


Figure 9. The proposed system in real life.

1. **Vehicle:** Currently, all vehicles are equipped with a central Electronic Control Unit (ECU) called the Gateway, which communicates with the Internet using a wireless module. Other functionalities include collecting data and initializing tests periodically. In addition, it is responsible for key exchange to establish secure communication between the vehicle and the OEM's server.
2. **Roadside Unit (RSU):** These are units located on the roadside that can be used to establish secure communication between the vehicle and the OEM servers. The RSU is considered a network path between the vehicles and the OEMs' servers and cannot modify or understand the data it receives as it receives encrypted data. They are of vital importance for the proposed system, as they are located everywhere along the road, and this makes vehicles able to communicate with servers whenever they need to send the collected data.
3. **OEMs' servers:** They play the role of miners, which are responsible for mining and validating the data, which is why the power consumption issue will not affect the vehicle as the mining process is performed on the server's side. We used OEMs' servers for mining, while in [34], they used the RSU, which is owned by the government. Thus, it is not considered a trusted solution. In addition, it will be very costly to add hardware components to each RSU. Using our solution, any vehicle with a specific brand can connect to its OEM servers and send the collected data. Each server can validate these data, and then, the consensus process is performed to decide the validity of the received data. If the data are valid, the block will be added to the Blockchain. The winning server will be responsible for adding this block to the chain, and the OEM can decide the rewards for the server agent. Another function of OEM servers is generating keys that will be used to secure and encrypt the data collected from the vehicle [35].
4. **Blockchain network:** We recommend using the consortium Blockchain type. As it is considered a private Blockchain with special access to a specific group, each OEM can create a group with specific access and settings. Furthermore, we recommend employing the PoW concept in the Blockchain. The aim of storing data in a Blockchain is that it is a standard way to have a secure and transparent process to validate and store vehicle data. In addition, it guarantees that the data will not be changed or modified by attackers. Therefore, we can monitor the vehicle's history and performance over the years. The above-mentioned advantages make our solution optimal for both users and OEMs. For users, they guarantee the correctness of their vehicle's performance in the event of selling it. OEMs can use these data to brand their vehicles. Figure 10 illustrates the sequence diagram of the proposed system.

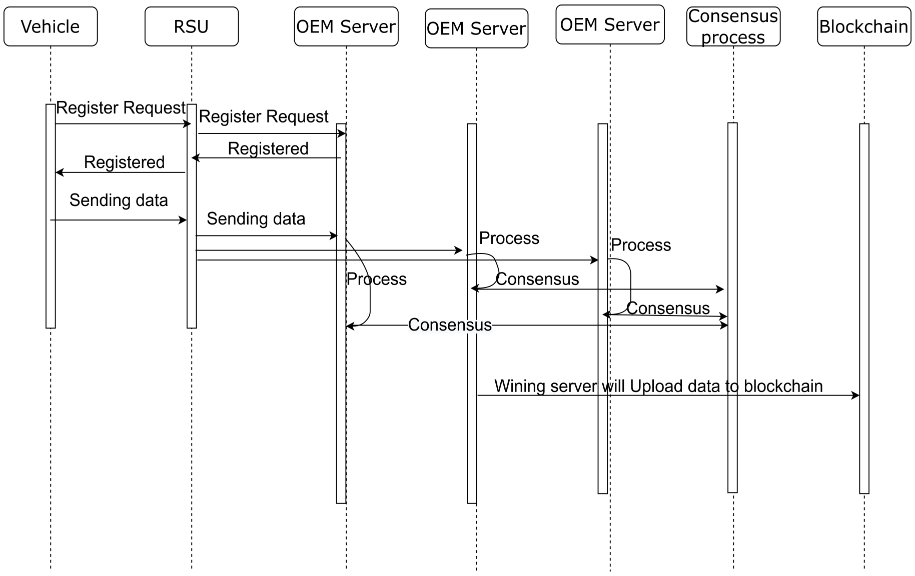


Figure 10. The sequence diagram of the proposed system.

4.2. Blockchain Implementation Architecture

The proposed system depends on collecting data from vehicles automatically to prevent adding any fake or false data in the case of manual entry. After production, the OEM should register the vehicle. At the start, the vehicle will read all parts' serial numbers using Data Identifiers (DIDs) to identify them. The DID is one of the services that Unified Diagnostic Services (UDS) supports to diagnose or request data from the vehicle using this number. The request sent to read the serial number should be as follows: (22 F1 40). This request should be sent to each ECU to read the serial number. The response should be as follows: (62 F1 40 + serial number). After this step, the system should check the originality of each part using the internal database or connect directly to the OEM's server. The second step is reading all the Data Trouble Codes (DTC). DTC is a code stored in an EPROM to indicate any problem. It is also one of the services supported by UDS-ISO. The third step is divided into three phases as follows:

1. Start self-tests for each part, and report the test result.
2. Read the production dates for each part using the DIDs. We can calculate the part's quality and lifetime from the previous two steps. Check the parts that have changed and their maintenance times.
3. Examine the car counter, and store it in the block. This is an important step because, in the used car market, this counter is reduced to a lower number, giving an incorrect indication of the car's usage time. The last step is reading the CO_2 emissions, which is important to maintain pollution within a certain limit and reduce it if necessary. In addition, a high emission of CO_2 indicates a problem with the motor. After gathering all this information, the block is ready to encrypt and sign. Then, after validating it, it will upload it to the Blockchain, where users and OEMs can browse and see the needed information. Figure 11 shows the flowchart of the proposed solution.

The collected data are divided into the following:

1. OEM report analysis: This is extracted from the stored data for one or more vehicles. The report contains information about the vehicle's reliability and the status of each component in terms of performance and originality. This kind of report is used to enhance the development process and provide the actual need for each market.
2. Timeline report analysis: This report gives a summary of the vehicle's status versus a specific time. It describes the defective parts, the time of replacement, the DTC recorded, and the causes of the defect.
3. Vehicle license, contract, traffic violation, and all legal papers that belong to this vehicle.

For example, car diagnostic codes, or DTCs, are made up of a five-digit alphanumeric code. The format is indicated in Figure 12.

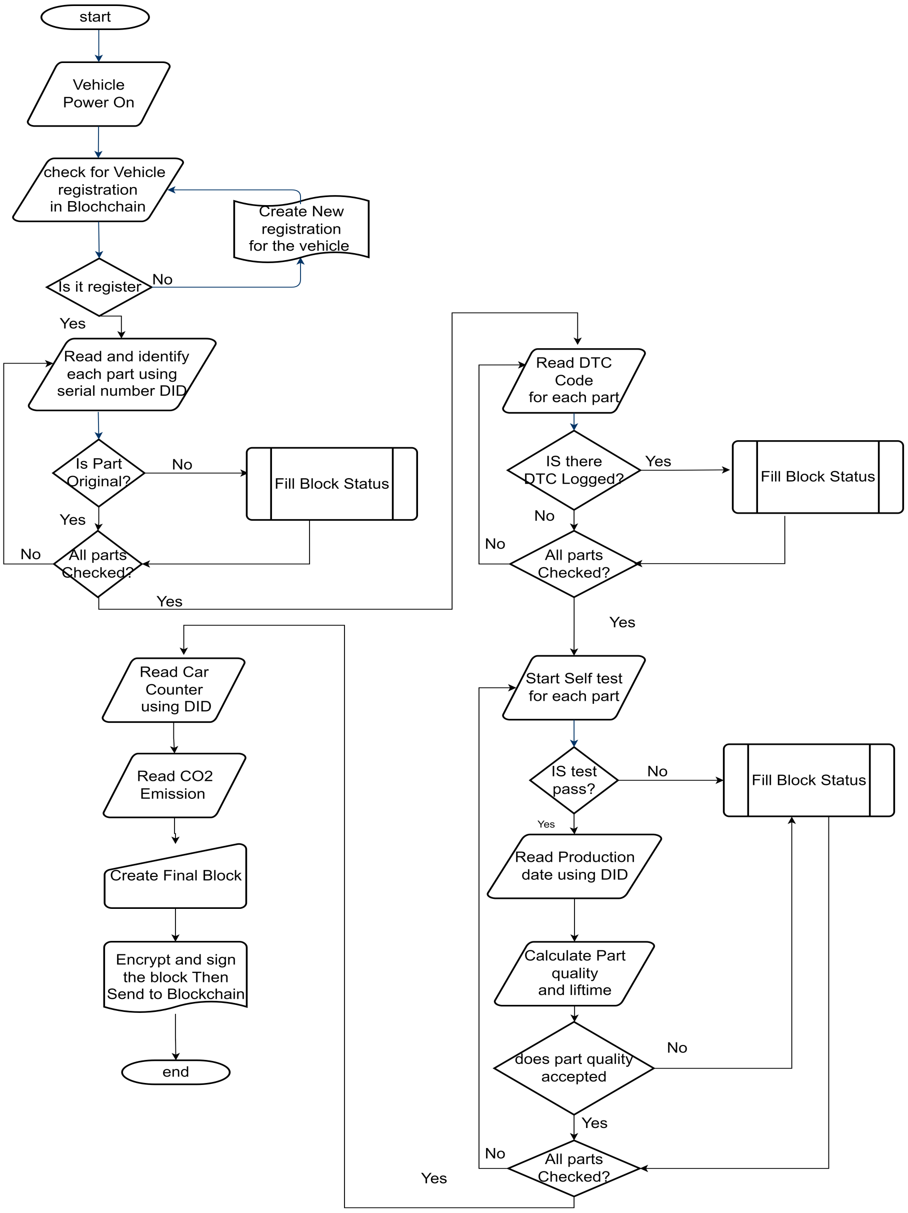

start
Vehicle Power On
check for Vehicle registration in Blochchain
Create New registration for the vehicle
Is it register
No
Yes
Read and identify each part using serial number DID
Is Part Original?
No
Fill Block Status
Yes
All parts Checked?
No
Yes
Read DTC Code for each part
IS there DTC Logged?
Yes
Fill Block Status
No
All parts Checked?
No
Yes
Start Self test for each part
IS test pass?
No
Fill Block Status
Yes
Read Production date using DID
Calculate Part quality and liftime
does part quality accepted
No
Yes
All parts Checked?
No
Yes
Read Car Counter using DID
Read CO2 Emission
Create Final Block
Encrypt and sign the block Then Send to Blockchain
end

Figure 11. The flowchart of the proposed system.

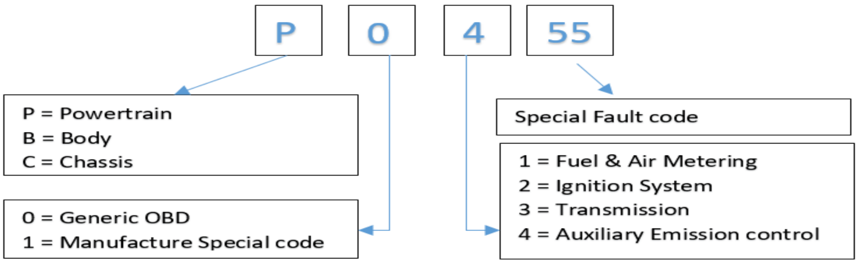


Figure 12. DTC interpretation.

4.3. Main Advantages of the Proposed Solution

As shown in Figure 13, the OEM and the owner can browse the data and analyze them. There are six main advantages concerning the OEM and vehicle owner's as follows:

- **Safety:** Avoids critical accidents due to any defect and alerts the user that the vehicle will make a safe shutdown if there is a serious problem.
- **Detect defective parts:** OEMs can detect the defective parts earlier and classify the defect based on the area. Correspondingly, it can take fast action by calling the vehicle faster or making a software update using FOTA.
- **Branding:** OEMs can use the results as reliable data when advertising their vehicles because the data extracted about the vehicle's performance have not been changed.
- **Analysis of part performance:** By analyzing part performance, OEMs can achieve faster solutions for better performance versus lifetime. In addition, this will increase the quality of some parts (i.e., air conditioning in hot areas).
- **Maintenance:** By saving maintenance and time, one will detect defective parts earlier and prevent damage to any parts connected to the defective one.
- **Vehicle history:** This is the most-useful feature, as users will have reliable data to use in the case of resale as a used vehicle, which increases trust in the vehicle's history.

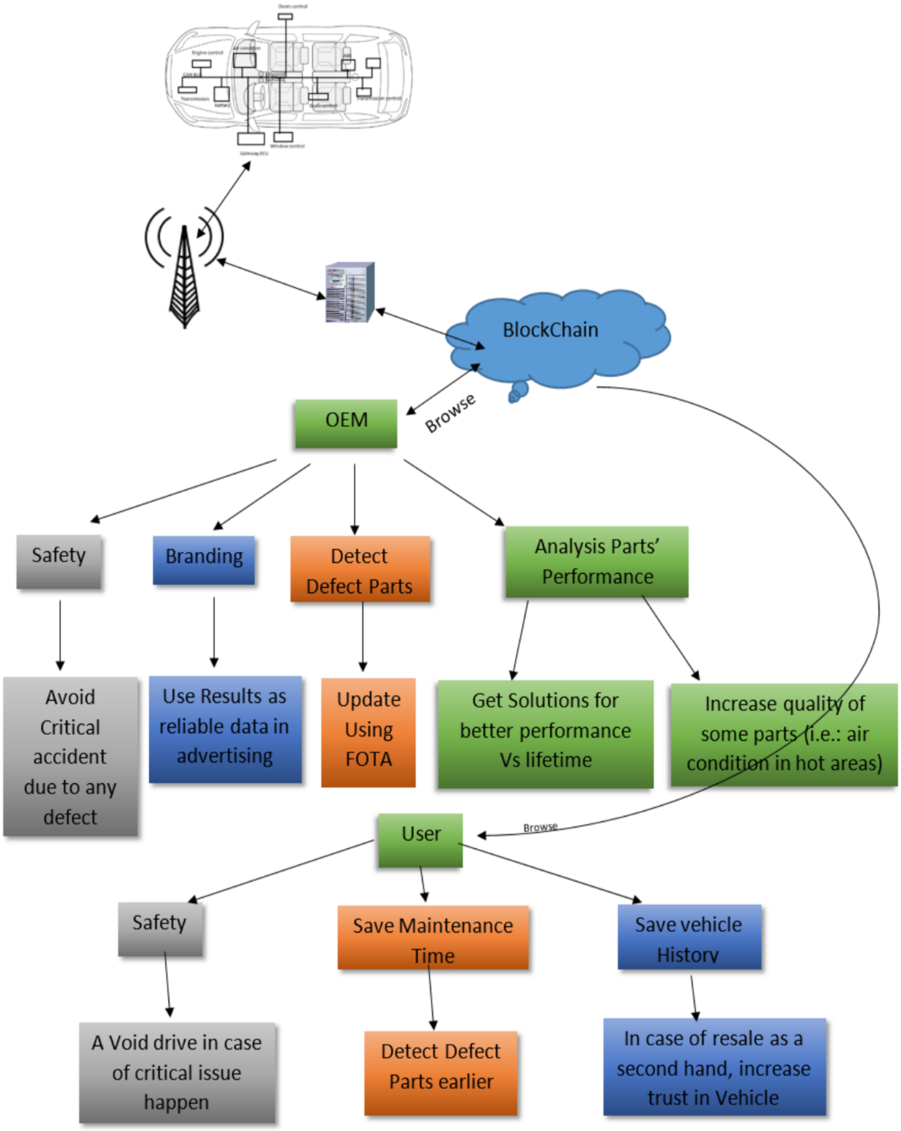

BlockChain
Browse
OEM
Safety
Branding
Detect Defect Parts
Analysis Parts' Performance
Avoid Critical accident due to any defect
Use Results as reliable data in advertising
Update Using FOTA
Get Solutions for better performance Vs lifetime
Increase quality of some parts (i.e.: air condition in hot areas)
Browse
User
Safety
Save Maintenance Time
Save vehicle History
A Void drive in case of critical issue happen
Detect Defect Parts earlier
In case of resale as a second hand, increase trust in Vehicle

Figure 13. The main benefits from the user and OEM's point of view.

5. Performance Evaluation and Security Analysis of the Proposed Solution

The performance evaluation via simulation is divided into four parts: vehicle simulation, Blockchain's simulation, a big view of the whole system (many vehicles to OEM server), and a use case sample.

5.1. Vehicle Simulation

The vehicle simulation in Figure 14 used MATLAB Version R2018b and the Simulink library. It is worth mentioning that MATLAB is a widely used simulation tool in the field of engineering and has several advantages:

- **User-friendly interface:** MATLAB has a user-friendly interface, which makes it easy to perform complex simulations and analyze the results.
- **Large community:** MATLAB has a large community of users who share their work and offer support through various forums and online communities.
- **Availability of toolboxes:** MATLAB provides various toolboxes that allow for the integration of multiple disciplines into a single simulation, making it a comprehensive and versatile tool.
- **Programming language:** MATLAB is based on a high-level programming language that allows for the customization of simulations and the development of new models.
- **Compatibility with other software:** MATLAB is compatible with other software, allowing for the integration of simulations into larger systems and workflows.

Overall, the advantages of using MATLAB are its versatility, ease of use, and availability of resources and toolboxes. However, depending on the specific needs of the simulation, other tools may also be suitable. Hence, this simulation is divided into the following: driver simulation, brake system simulation, motor simulation, battery simulation, driveline simulation, and fault detection system simulation. In our simulation, we considered two parameters as the main factors:

(1) Battery status: If the battery values obtained from the simulator are below 60%, then we have a battery fault with DTC P406.
(2) Temperature status: Temperatures are tested while the vehicle is running. For values greater than a certain value, we have a battery fault with DTC P405.

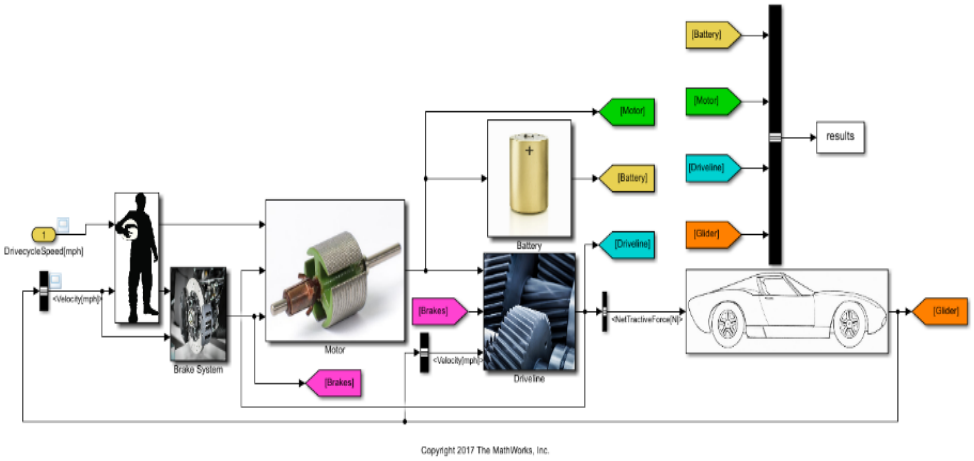


Figure 14. A simulation of a vehicle sending with periodic rate to the Blockchain using MATLAB.

Some results from the vehicle's simulation include the battery's state of charge and power consumption versus the vehicle's speed. Figure 15 illustrates the battery's State of Charge (SoC); Figure 16 shows the power consumption versus the vehicle's speed; Figure 17 represents the battery simulation inside the vehicle, which decays to 65% in 60 seconds. We edited some parameters to make the battery decay faster due to the limitations of the simulation time and processing.

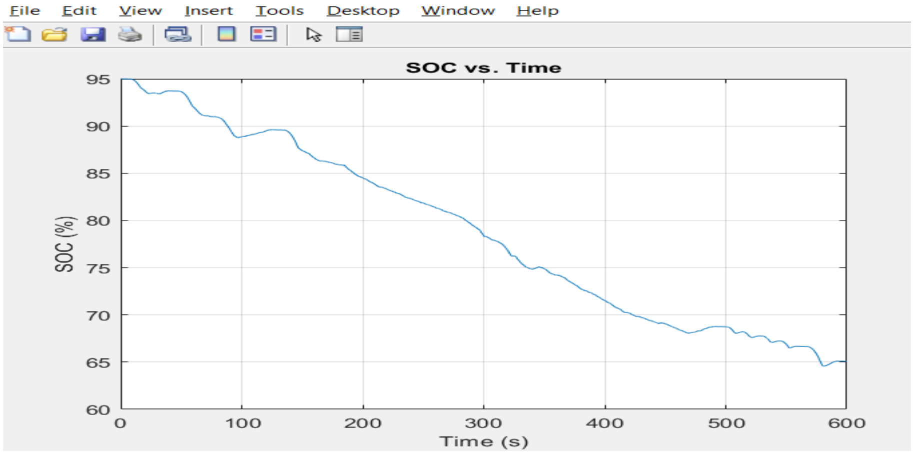


Figure 15. Battery's State of Charge (SoC).

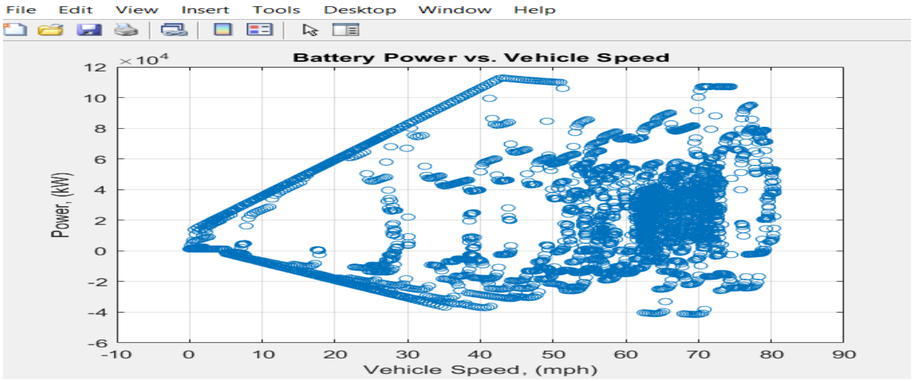


Figure 16. Power consumption versus vehicle's speed.

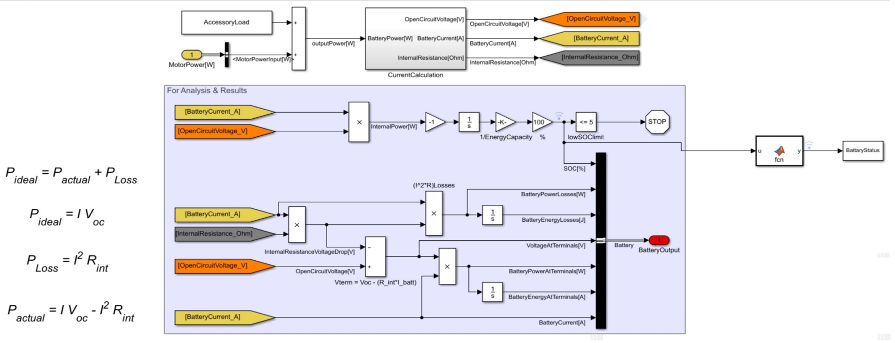


Figure 17. Battery simulation in the proposed system.

5.2. Blockchain Simulation

The Blockchain simulation is divided into the Blockchain initialization and the Blockchain core script. The Blockchain initialization is responsible for initializing the Blockchain and creating the genesis block, as shown in Figures A1 and A2 (see Appendix A). On the other hand, the Blockchain core script is responsible for collecting the data and validating them, as illustrated in Figure A3. In the event of a fault, an indication LED displays the existing fault, as shown in Figure A4. Figures A5 and A6 show the code used in the validation and the saving of the data in the case of valid data inside the Blockchain. Finally, Figure A7 illustrates the final content of the Blockchain after several runs.

5.3. Overall System Performance

The simulation of a system containing several vehicles sending packets to a server was performed using OMNET++, which provides several advantages. First, it allows for the modeling of realistic network topologies and communication scenarios, enabling a thorough evaluation of the system's performance under different conditions. Second, OMNET++ provides a high level of flexibility and control over the simulation parameters, enabling the simulation of various system configurations and scenarios. Finally, OMNET++ provides a wide range of statistical analysis tools for the results obtained from the simulations, allowing for a detailed analysis and comparison of the system's performance under different conditions. In summary, the use of OMNET++ to evaluate the proposed continuous monitoring system based on Blockchain technology enables a more realistic and thorough evaluation of the system's performance, providing valuable insights into its effectiveness and identifying areas for improvement. Accordingly, the aim of the simulation was to give some expectations about the needed storage, the sending periodicity for each vehicle, and the expected throughput for specific communication speeds. Table 3 shows the simulation setup for OMNET++. Figure 18 depicts a system of twelve vehicles sending messages to one OEM server.

Table 3. Simulation setup for OMNET++.

Parameter	Value
Simulator	OMNET++
Number of vehicles	6 or 12 or 24
Simulation time	60 s
Simulation area	500 m × 650 m
Packet size	1000 Byte
Communication range	1000 m
Bit rate	2 Mbps
Channel type	Wireless
Send interval	1 s [1]

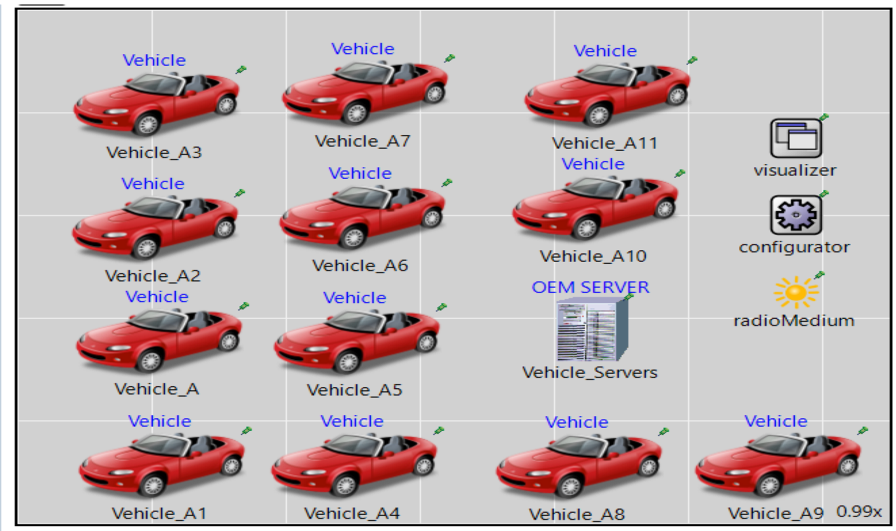


Figure 18. Full setup for 12 vehicles sending 1000 bytes to the OEM server.

As shown in Figure 19, the system's throughput increases as the number of vehicles increases. Figure 20 illustrates that the residual energy stored decreases faster by increasing the number of vehicles. In addition, as shown in Figure 21, the end-to-end delay increases by increasing the number of vehicles. In addition, power consumption increases by increasing the number of vehicles, as shown in Figure 22. These results give us an in-depth understanding of the network's shape and the expected throughputs and the needed storage and power consumption given the number of participating vehicles. In general, OEMs can implement this system by either increasing the storage to add more vehicles to the system or decreasing the sending frequency to allow more vehicles to join. Therefore, the system is fully dynamic, and its configuration can be adjusted to satisfy the OEM's needs. There are no specific constraints when implementing it.

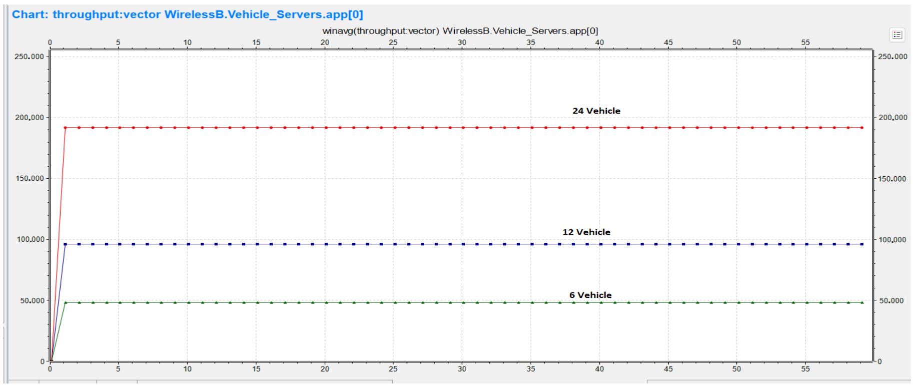


Figure 19. System's throughputs for 6, 12, and 24 vehicles.

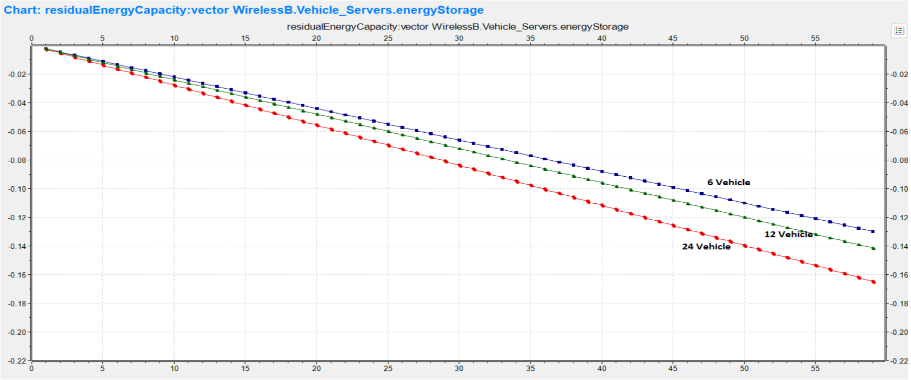


Figure 20. Residual energy stored for 6, 12, and 24 vehicles.

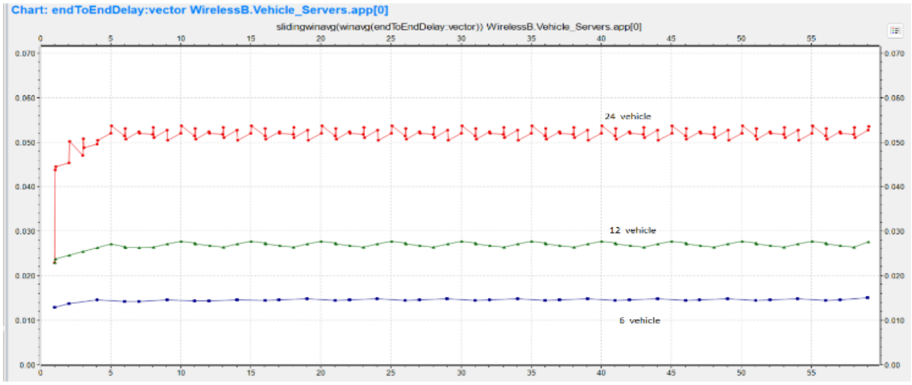


Figure 21. End-to-end delay for 6, 12, and 24 vehicles.

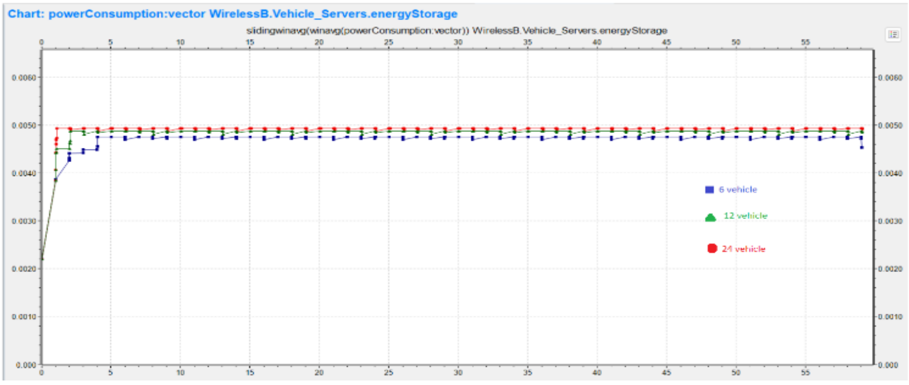


Figure 22. The power consumption for 6, 12 and 24 vehicles.

5.4. Use Case Scenario

The analysis is divided into the analysis of logged DTC over time and the analysis of the performance of specific parts. As shown in Figure 23, the analysis of logged DTC over time provides an automatic and clear vehicle history over time with trusted results for all issues in the vehicle throughout its history. As shown in Figures 24 and 25, an analysis of the performance of specific parts is used to assess the vehicle's parts over time (for example, the state of charge for the battery over time).

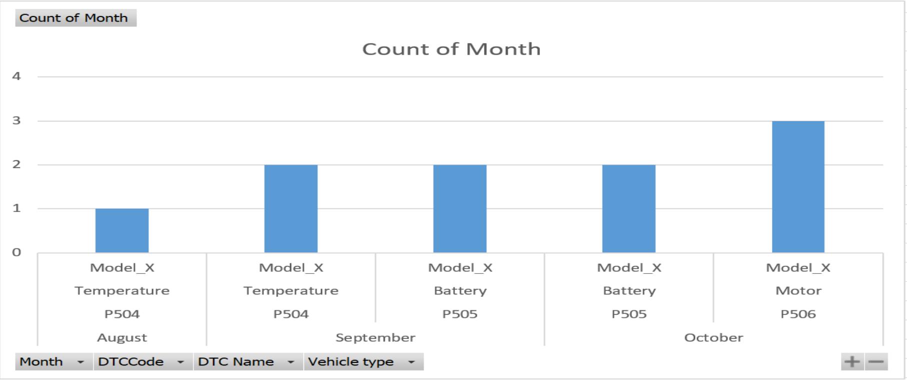
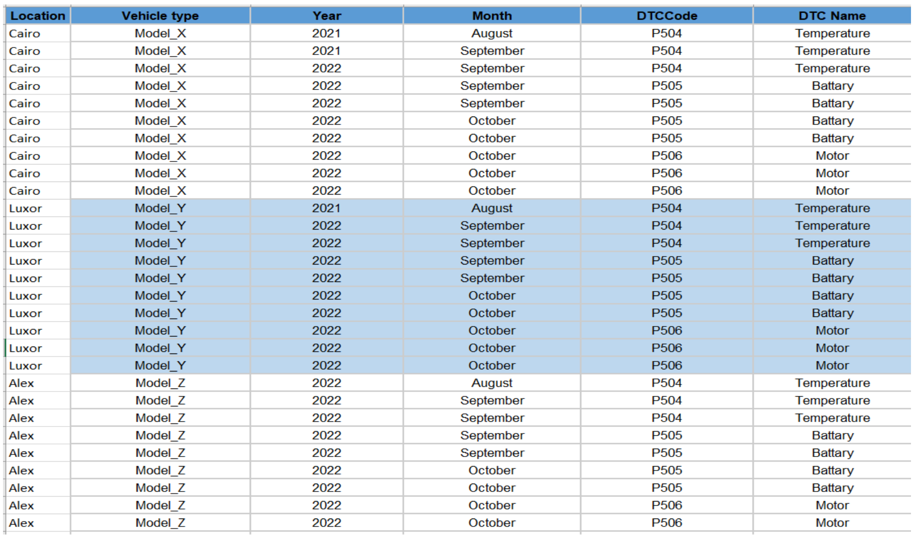


Figure 23. The history for one vehicle and all its logged DTC with timeline (used by vehicle's user for analysis of performance).



Location	Vehicle type	Year	Month	DTCCode	DTC Name
Cairo	Model_X	2021	August	P504	Temperature
Cairo	Model_X	2021	September	P504	Temperature
Cairo	Model_X	2022	September	P504	Temperature
Cairo	Model_X	2022	September	P505	Battary
Cairo	Model_X	2022	September	P505	Battary
Cairo	Model_X	2022	October	P505	Battary
Cairo	Model_X	2022	October	P505	Battary
Cairo	Model_X	2022	October	P506	Motor
Cairo	Model_X	2022	October	P506	Motor
Cairo	Model_X	2022	October	P506	Motor
Luxor	Model_Y	2021	August	P504	Temperature
Luxor	Model_Y	2022	September	P504	Temperature
Luxor	Model_Y	2022	September	P504	Temperature
Luxor	Model_Y	2022	September	P505	Battary
Luxor	Model_Y	2022	September	P505	Battary
Luxor	Model_Y	2022	October	P505	Battary
Luxor	Model_Y	2022	October	P505	Battary
Luxor	Model_Y	2022	October	P506	Motor
Luxor	Model_Y	2022	October	P506	Motor
Luxor	Model_Y	2022	October	P506	Motor
Alex	Model_Z	2022	August	P504	Temperature
Alex	Model_Z	2022	September	P504	Temperature
Alex	Model_Z	2022	September	P504	Temperature
Alex	Model_Z	2022	September	P505	Battary
Alex	Model_Z	2022	September	P505	Battary
Alex	Model_Z	2022	October	P505	Battary
Alex	Model_Z	2022	October	P505	Battary
Alex	Model_Z	2022	October	P506	Motor
Alex	Model_Z	2022	October	P506	Motor

Figure 24. The report extracted from the Blockchain for many vehicle model and all logged DTC with timeline and location.

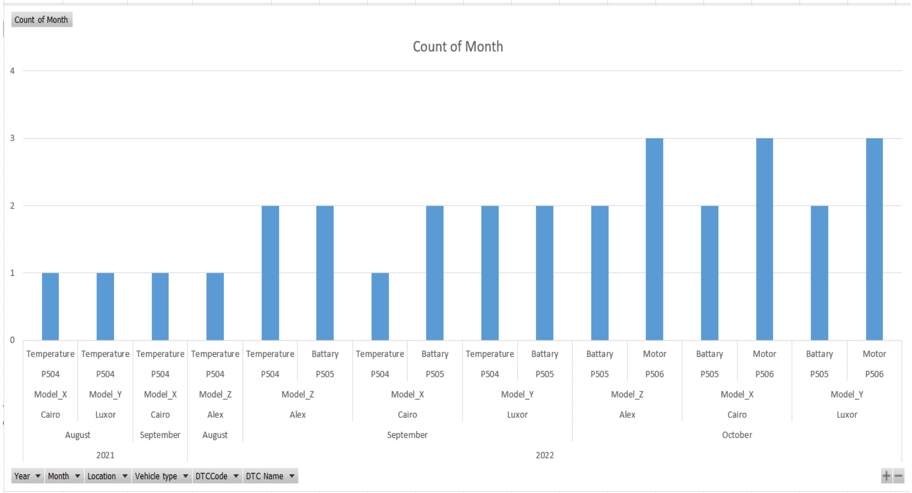


Figure 25. The history for many vehicle models and all logged DTC with timeline (used by the OEM for analysis of performance).

To summarize, the main advantages of developing a Blockchain-based fully automated solution for remote automatic vehicle diagnosis are:

1. **Increased security:** Blockchain technology provides a secure and immutable ledger that can be used to store data related to vehicle diagnostics. This ensures that the data are not tampered with or manipulated in any way.
2. **Improved efficiency:** By automating the process of vehicle diagnosis, the system can quickly identify any issues and provide solutions in a timely manner. This reduces the time and cost associated with manual diagnosis.
3. **Enhanced transparency:** The Blockchain-based system allows for greater transparency as all data related to vehicle diagnostics are stored on an immutable ledger. This ensures that all parties involved have access to accurate information about the vehicle's condition at all times.
4. **Reduced fraud:** By verifying each part's originality, the system can help reduce fraud and ensure that only genuine parts are used in repairs or replacements.

Finally, Table 4 provides a qualitative and quantitative comparison between the proposed and existing systems.

Table 4. Feature/performance comparison between the proposed and existing systems.

Feature/Performance	Proposed System	[29]	[30]	[31]	[32]	[33]
Automatic collecting data	Yes	Yes	No	No	No	No
Embedded inside vehicle	Yes	Yes	No	No	No	No
Confidentiality	Yes	No	No	Yes	No	Yes
Authentication	Yes	No	No	Yes	Yes	Yes
Encryption	Yes	No	No	Yes	Yes	Yes
Integrity	Yes	No	No	Yes	Yes	Yes
Throughput	Medium	Low	High	Low	Low	Low
Periodicity	High	High	N/A	N/A	N/A	N/A
Configurable	High	Low	Medium	Low	Low	Low
Self-check on all system	High	Low	Low	Low	Low	Low

5.5. Real-World Testing

The proposed system in the paper is based on Blockchain technology to provide secure and trusted storage and verification of vehicle data. Here are some steps that could be taken to implement the Blockchain network in this system:

1. Develop and deploy the system: The first step would be to develop the system and deploy it on a test network. This would involve designing and coding the software, setting up the network infrastructure, and configuring the system to work with the OEM's servers. Here are some steps that could be taken to implement the Blockchain network in this system:
   i. Determine the type of Blockchain: There are different types of Blockchain, including public, private, and consortium. For this system, a private or consortium Blockchain might be more suitable, as it allows the OEM to have more control over the network.
   ii. Choose a consensus mechanism: The consensus mechanism is used to validate transactions and add new blocks to the Blockchain. Popular consensus mechanisms include the Proof of Work (PoW) and Proof of Stake (PoS). The paper suggests using the PoW, but other mechanisms might be more appropriate depending on the specific requirements of the system.
   iii. Design the smart contract: A smart contract is a self-executing program that runs on the Blockchain and enforces the rules of the system. In this case, the smart contract could define the data structure for storing vehicle information, as well as the rules for validating and adding new blocks to the Blockchain.
   iv. Set up the network: Once the Blockchain parameters are defined, the network can be set up using the chosen Blockchain platform. This might involve setting up nodes, deploying the smart contract, and configuring the consensus mechanism.
   v. Integrate with the vehicle: The vehicle must be able to communicate with the Blockchain network in order to send data and receive updates. This might involve installing special hardware or software on the vehicle, such as a telematics device or an onboard computer.
2. Testing the system: After deploying the system, it would need to be thoroughly tested to ensure that it works as expected. This would involve testing its ability to monitor vehicle performance, collect and store data securely, and communicate with the OEM's servers. For testing the system in real life, testing is divided into the following:
   i. Testing the designed data block, which is extracted automatically after the vehicle runs self-testing code.
   ii. Testing the encryption processing.
   iii. Despite the data being encrypted, secure communication should be applied while sending data to the Blockchain.
   iv. Testing the mining processing in the OEM's server.
   v. Designing and testing the storage strategy to fit the increasing number of vehicles.
3. Piloting the system: Once the system has been tested and any issues have been addressed, it can be piloted on a small scale to test its effectiveness in the real-world. This could involve deploying the system in a limited geographic area or with a small group of vehicles.
4. Scaling up the system: If the pilot is successful, the system can be scaled up to cover a larger geographic area or a larger number of vehicles. This would involve expanding the network infrastructure and adding additional hardware and software as needed.
5. Ongoing maintenance and updates: Once the system is deployed and in use, ongoing maintenance and updates will be required to ensure that it continues to function effectively and securely. This would involve monitoring the system for issues, making updates and upgrades as needed, and addressing any security concerns that arise.

Overall, implementing and testing such a system in the real-world would require a significant investment of time and resources, as well as careful planning and coordination between the OEM, network providers, and other stakeholders involved in the project.

5.6. Assumption and Limitations

Table 5 lists all used abbreviations in this work. Also, there are some assumptions and limitations that should be taken into account as follows:

Assumptions:

- The proposed system assumes that all vehicles have a built-in communication module capable of communicating with the manufacturer′s servers.
- The system assumes that the manufacturer′s servers are always available and can handle the incoming data from all the connected vehicles.
- The simulation results are assumed to be representative of real-world performance and throughput, and any changes in the parameters or network conditions may affect the actual results.
- The proposed system assumes that all the vehicles in the network are authenticated and authorized to participate in the system.
- The communication between a vehicle and the OEM's server is secured using a symmetric key saved inside the vehicle board inside the memory of the Hardware Security Module (HSM).
- The data transmitted between the vehicle and OEM server are first encrypted using a symmetric key shared between the OEM and vehicle. Data should be signed using the private key of the vehicle.
- Security and integrity are maintained through the Blockchain.

Limitations:

- The proposed system requires a significant investment in infrastructure and hardware to implement and maintain. System engineers can design the shape of the data and the sending periodicity to optimize this limitation.
- The system may face scalability issues as the number of vehicles in the network increases, which may require additional resources to be allocated to maintain the system's performance. The results showed that OEMs can implement this system by considering whether to increase storage to add more vehicles to the system or decrease the sending periodicity to allow more vehicles to join.
- The system relies on the availability and reliability of the Internet connection, which may be affected by various factors such as network congestion, weather conditions, or maintenance work.
- The system's security relies heavily on the encryption algorithms used and the effectiveness of the Blockchain technology. Any vulnerabilities or weaknesses in these components may compromise the system's security and integrity.
- The system may face regulatory challenges as it deals with personal and sensitive data, and compliance with data protection regulations such as GDPR must be ensured.

Table 5. List of all used abbreviations.

Abbreviation	Expression
HSM	Hardware Security Module
OEM	Original Equipment Manufacturer
DTCs	Diagnostic Trouble Codes
FOTA	Flash Over The Air
PoW	Proof of Work
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PoET	Proof of Elapsed Time
PoA	Proof of Activity
PoC	Proof of Capacity
OBD	On-Board Diagnostics
ECU	Electronic Control Unit
RSU	Roadside Unit
DIDs	Data Identifiers
UDS	Unified Diagnostic Services
SoC	State of Charge

6. Conclusions and Future Work

The current structure of the automotive industry suffers from a lack of continuous monitoring regarding the information on the internal performance of the vehicle and the status of the internal parts. Most of the previous solutions presented a manual solution to monitor the vehicle's performance and errors, which requires human interaction. This may lead to adding false information, either accidentally or intentionally.

In this work, we proposed a solution for remote automatic vehicle diagnosis. Our system is fully automated. The main principles of the system are to periodically check all logged DTC in the vehicle, check each part's performance, and check the originality of each part. Then, the system constructs a block to send to the vehicle manufacturer's servers. Those servers act as validators to validate these data and make sure that no hacking or false data insertion occurs. Next, the OEM servers execute the PoW consensus mechanism. After validation, the block is inserted into the Blockchain with the entire vehicle's information. Because no data inside the Blockchain can be modified, the data stored in the Blockchain can be used by the vehicle's owner to check the vehicle's performance, determine the required maintenance time to avoid a critical accident, and provide proof of the vehicle's history in the case of resale. The manufacturer can use these data to analyze the vehicle's performance in different environments and weather conditions; in addition, they can enhance the performance, if needed, by improving the software and upgrading it remotely using FOTA. Furthermore, the main benefit is that they can advertise their product using reliable data extracted from a trusted source, such as the Blockchain. Furthermore, given real data from previous experience, the dependability and performance of all brands can be measured.

In order to meet the minimal requirements, the system was simulated using MATLAB to simulate the vehicles and the Blockchain. In addition, the network was simulated using OMNET++ to measure the expected storage and throughputs for some fixed parameters, such as sending the periodicity and speed and the maximum number of vehicles. The results showed that OEMs can implement this system by taking into consideration whether to increase storage to add more vehicles to the system or decrease the sending periodicity to allow more vehicles to join. Therefore, the system is fully dynamic, and its configuration can be adjusted to satisfy the OEM's needs. There are no specific constraints when implementing it.

Finally, these are some possible directions for future work to enhance the proposed system:

1. **Integration with Artificial Intelligence (AI):** One potential direction for future work is to integrate the proposed system with AI techniques, such as machine learning, to improve the accuracy and efficiency of the diagnostic and maintenance processes. This could involve using AI to analyze the data collected from the vehicles to identify patterns and anomalies and to make predictions about future maintenance needs. For example, AI techniques can be used to train autonomous cars using the data stored in the Blockchain, then testing the developed algorithm using real data [15].
2. **Privacy and security:** As with any system that collects and stores sensitive data, privacy and security will be a critical concern for the proposed approach. Future work could focus on developing and testing robust security mechanisms to protect the data collected by the system and to ensure that only authorized parties have access to them. Furthermore, formal methods and techniques can be used to provide a rigorous approach to analyzing the security of the proposed system [36].
3. **Automatic firmware update:** The proposed system can be enhanced for updating FOTA to avoid the attacks that target the network during the software update [37].
4. **Scalability:** The proposed system will need to be able to scale to accommodate large numbers of vehicles and users. Future work could explore ways to optimize the system's performance and scalability, such as through the use of distributed ledger technologies or other approaches [38].
5. **Integration with public transport systems:** Finally, another potential direction for future work is to explore the integration of the proposed system with public transport

systems, such as buses and trains. This could enable real-time monitoring of vehicle performance and maintenance needs and could also help to improve the overall efficiency and reliability of public transport services [14].

Author Contributions: Conceptualization, H.K.A. and I.T.A.H.; methodology, H.K.A. and I.T.A.H.; software, A.M.Y.; validation, A.M.Y., H.K.A. and I.T.A.H.; formal analysis, I.T.A.H. and A.M.Y.; investigation, H.K.A. and A.M.Y.; resources, A.M.Y., H.K.A. and I.T.A.H.; data curation, A.M.Y., H.K.A. and I.T.A.H.; writing—original draft preparation, A.M.Y.; writing—A.M.Y., H.K.A. and I.T.A.H.; visualization, A.M.Y.; supervision, H.K.A. and I.T.A.H.; project administration, H.K.A. and I.T.A.H.; funding acquisition, A.M.Y. All authors have read and agreed to the published version of the manuscript.

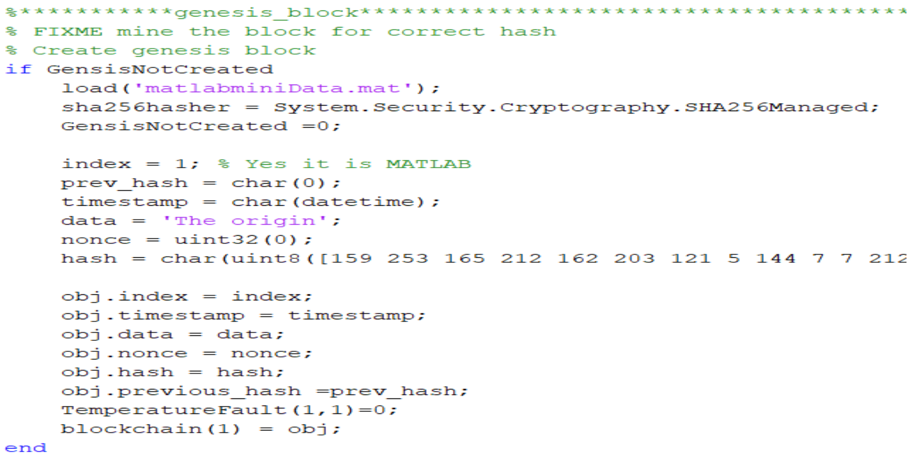
Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to acknowledge VALEO Inter-branch Automotive Software and Nile University, Egypt.

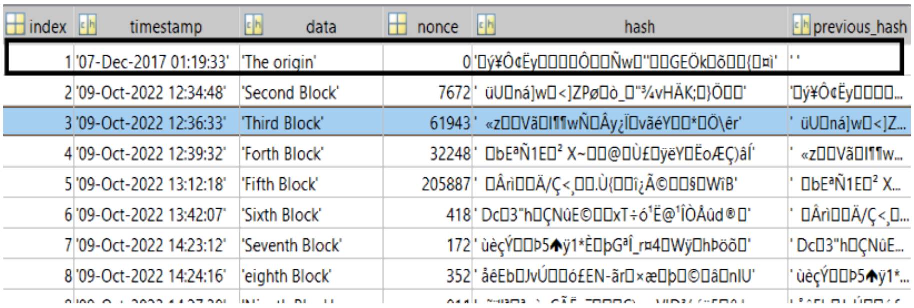
Conflicts of Interest: The authors declare no conflict of interest.

Appendix A



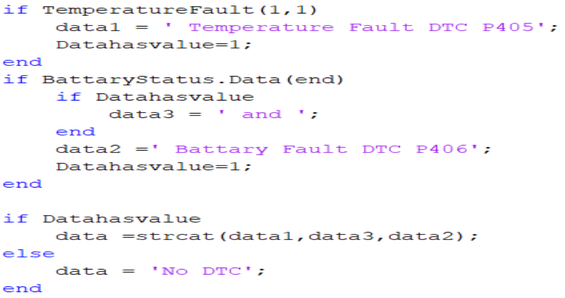
```
%***********genesis_block****************************************
% FIXME mine the block for correct hash
% Create genesis block
if GensisNotCreated
    load('matlabminiData.mat');
    sha256hasher = System.Security.Cryptography.SHA256Managed;
    GensisNotCreated =0;

    index = 1; % Yes it is MATLAB
    prev_hash = char(0);
    timestamp = char(datetime);
    data = 'The origin';
    nonce = uint32(0);
    hash = char(uint8([159 253 165 212 162 203 121 5 144 7 7 212

    obj.index = index;
    obj.timestamp = timestamp;
    obj.data = data;
    obj.nonce = nonce;
    obj.hash = hash;
    obj.previous_hash =prev_hash;
    TemperatureFault(1,1)=0;
    blockchain(1) = obj;
end
```

Figure A1. The code checking the creation of the genesis block.



index	timestamp	data	nonce	hash	previous_hash
1	'07-Dec-2017 01:19:33'	'The origin'	0	'□ý¥Ô¢Ëy□□□□Ô□□Ñw□"□□GEÖk□õ□□{□¤ì'	' '
2	'09-Oct-2022 12:34:48'	'Second Block'	7672	' üU□ná]w□<]ZPø□ò_□"¾vHÄK;□}Ö□□'	'□ý¥Ô¢Ëy□□□□...
3	'09-Oct-2022 12:36:33'	'Third Block'	61943	' «z□□Vã□I¶¶wÑ□Ây¿Ï□vãéY□□*□Ö\êr'	' üU□ná]w□<]Z...
4	'09-Oct-2022 12:39:32'	'Forth Block'	32248	' □bEªÑ1E□² X~□□@□Ù£□ÿëY□ËoÆÇ)âÍ'	' «z□□Vã□I¶¶w...
5	'09-Oct-2022 13:12:18'	'Fifth Block'	205887	' □Âri□□Ä/Ç<¸□□.Ù{□□ì¿Ã©□□§□WîB'	' □bEªÑ1E□² X...
6	'09-Oct-2022 13:42:07'	'Sixth Block'	418	' Dc□3"h□ÇNûE©□□xT÷ó¹Ë@¹ÎÒÅûd®□'	' □Âri□□Ä/Ç<¸□...
7	'09-Oct-2022 14:23:12'	'Seventh Block'	172	' ùèçÝ□□Þ5🡅ÿ1*È□þGªÎ_r¤4□Wÿ□hÞöõ□'	' Dc□3"h□ÇNûE...
8	'09-Oct-2022 14:24:16'	'eighth Block'	352	' åêEb□JvÚ□□ó£EN-ãr□×æ□þ□©□â□nIU'	' ùèçÝ□□Þ5🡅ÿ1*...
9	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Figure A2. Shape of genesis block in the Blockchain.



```
if TemperatureFault(1,1)
    data1 = ' Temperature Fault DTC P405';
    Datahasvalue=1;
end
if BattaryStatus.Data(end)
    if Datahasvalue
        data3 = ' and ';
    end
    data2 =' Battary Fault DTC P406';
    Datahasvalue=1;
end

if Datahasvalue
    data =strcat(data1,data3,data2);
else
    data = 'No DTC';
end
```

Figure A3. The code used in collecting data.

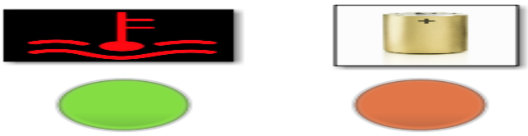
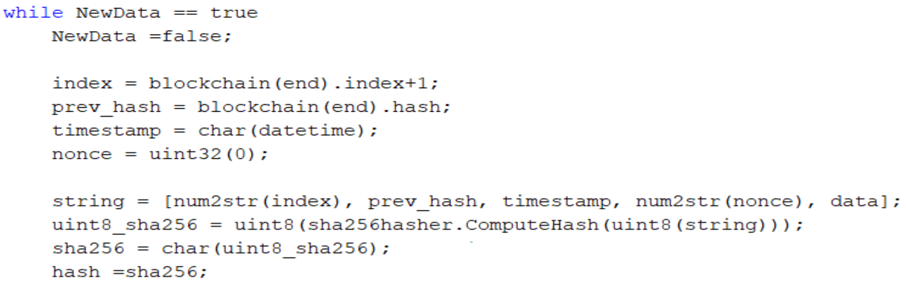
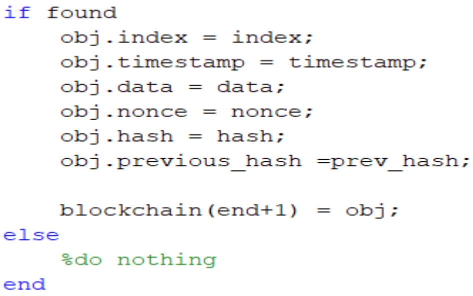


Figure A4. The status of tested parts in the system.



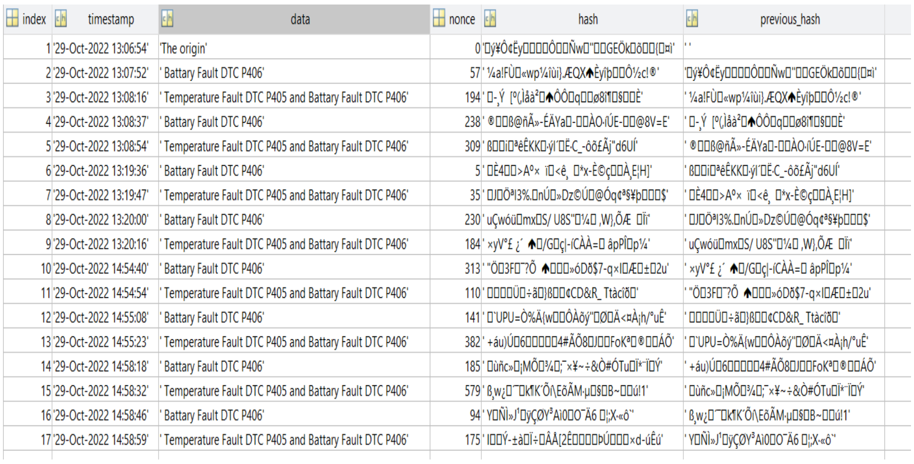
```
while NewData == true
    NewData =false;

    index = blockchain(end).index+1;
    prev_hash = blockchain(end).hash;
    timestamp = char(datetime);
    nonce = uint32(0);

    string = [num2str(index), prev_hash, timestamp, num2str(nonce), data];
    uint8_sha256 = uint8(sha256hasher.ComputeHash(uint8(string)));
    sha256 = char(uint8_sha256);
    hash =sha256;
```

Figure A5. The code used in data validation.



```
if found
    obj.index = index;
    obj.timestamp = timestamp;
    obj.data = data;
    obj.nonce = nonce;
    obj.hash = hash;
    obj.previous_hash =prev_hash;

    blockchain(end+1) = obj;
else
    %do nothing
end
```

Figure A6. The code used to save data inside the Blockchain in the case of receiving valid data.



index	timestamp	data	nonce	hash	previous_hash
1	'29-Oct-2022 13:06:54'	'The origin'	0	'□ý¥Ô¢Ëy□□□□Ô□□Ñw□"□□GEÖk□õ□□{□¤ì'	' '
2	'29-Oct-2022 13:07:52'	' Battary Fault DTC P406'	57	' ¼a!FÙ□«wp¼îùi}.ÆQX⬆Èyîþ□□Ô½c!®'	'□ý¥Ô¢Ëy□□□□Ô□□Ñw□"□□GEÖk□õ□□{□¤ì'
3	'29-Oct-2022 13:08:16'	' Temperature Fault DTC P405 and Battary Fault DTC P406'	194	' □-¸Ý [º(,Ìåà²□⬆ÔÔ□q□□ø8î¶□§□□È'	' ¼a!FÙ□«wp¼îùi}.ÆQX⬆Èyîþ□□Ô½c!®'
4	'29-Oct-2022 13:08:37'	' Battary Fault DTC P406'	238	' ®□□ß@ñÃ»-ÉÄYa□-□□ÀO·íÚE-□□@8V=E'	' □-¸Ý [º(,Ìåà²□⬆ÔÔ□q□□ø8î¶□§□□È'
5	'29-Oct-2022 13:08:54'	' Temperature Fault DTC P405 and Battary Fault DTC P406'	309	' ß□□i□ªêÊKK□·ýl´□Ë·C_-ôõ£Ãj"d6UÍ'	' ®□□ß@ñÃ»-ÉÄYa□-□□ÀO·íÚE-□□@8V=E'
6	'29-Oct-2022 13:19:36'	' Battary Fault DTC P406'	5	' □È4□□>Aº× ï□<ê¸ □*x-È©ç□□À¸E¦H]'	' ß□□i□ªêÊKK□·ýl´□Ë·C_-ôõ£Ãj"d6UÍ'
7	'29-Oct-2022 13:19:47'	' Temperature Fault DTC P405 and Battary Fault DTC P406'	35	' □J□Öªl3%.□nÚ□»Dz©Ú□@Óq¢ª§¥þ□□□$'	' □È4□□>Aº× ï□<ê¸ □*x-È©ç□□À¸E¦H]'
8	'29-Oct-2022 13:20:00'	' Battary Fault DTC P406'	230	' uÇwóü□mx□S/ U8S"□¼□ ,W},ÕÆ □Ïï'	' □J□Öªl3%.□nÚ□»Dz©Ú□@Óq¢ª§¥þ□□□$'
9	'29-Oct-2022 13:20:16'	' Temperature Fault DTC P405 and Battary Fault DTC P406'	184	' ×yV°£ ¿´ ⬆□/G□ç|-íCÀÀ=□ âpPÎ□p¼'	' uÇwóü□mx□S/ U8S"□¼□ ,W},ÕÆ □Ïï'
10	'29-Oct-2022 14:54:40'	' Battary Fault DTC P406'	313	' "Ö□3F□¯?Õ ⬆□□□»óDð$7-q×I□Æ□±□2u'	' ×yV°£ ¿´ ⬆□/G□ç|-íCÀÀ=□ âpPÎ□p¼'
11	'29-Oct-2022 14:54:54'	' Temperature Fault DTC P405 and Battary Fault DTC P406'	110	' □□□□Ü□÷ã□}ß□□¢CD&R_ Ttàcîð□'	' "Ö□3F□¯?Õ ⬆□□□»óDð$7-q×I□Æ□±□2u'
12	'29-Oct-2022 14:55:08'	' Battary Fault DTC P406'	141	' □`UPU=Ò%Ä{w□□ÔÀõý"□Ø□Ä<¤À¡h/°uÊ'	' □□□□Ü□÷ã□}ß□□¢CD&R_ Ttàcîð□'
13	'29-Oct-2022 14:55:23'	' Temperature Fault DTC P405 and Battary Fault DTC P406'	382	' +áu)Ú□6□□□□□4#ÃÕ8□J□□FoKª□®□□ÁÕ'	' □`UPU=Ò%Ä{w□□ÔÀõý"□Ø□Ä<¤À¡h/°uÊ'
14	'29-Oct-2022 14:58:18'	' Battary Fault DTC P406'	185	' □ùñc»□¡MÕ□¾□;¯×¥~÷&Ò#ÓTu□Ï*¨Ï□Ý'	' +áu)Ú□6□□□□□4#ÃÕ8□J□□FoKª□®□□ÁÕ'
15	'29-Oct-2022 14:58:32'	' Temperature Fault DTC P405 and Battary Fault DTC P406'	579	' ß¸w¿□¯□k¶K´Õí\EõÃM·µ□§□B~□□ú!1'	' □ùñc»□¡MÕ□¾□;¯×¥~÷&Ò#ÓTu□Ï*¨Ï□Ý'
16	'29-Oct-2022 14:58:46'	' Battary Fault DTC P406'	94	' Y□ÑÌ»J¹□ÿÇØY³Aì0□O¯Ä6 □¦;X·«ô`'	' ß¸w¿□¯□k¶K´Õí\EõÃM·µ□§□B~□□ú!1'
17	'29-Oct-2022 14:58:59'	' Temperature Fault DTC P405 and Battary Fault DTC P406'	175	' I□□Ý-±à□Ï÷□ÂÅ[2Ê□□□□ÞÚ□□□×d-úÊú'	' Y□ÑÌ»J¹□ÿÇØY³Aì0□O¯Ä6 □¦;X·«ô`'

Figure A7. The final content of Blockchain after several runs.

References

1. Masood, A.; Lakew, D.S.; Cho, S. Security and privacy challenges in connected vehicular cloud computing. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2725–2764. [CrossRef]
2. Wu, L.; Zhang, R.; Li, Q.; Ma, C.; Shi, X. A mobile edge computing-based applications execution framework for Internet of Vehicles. *Front. Comput. Sci.* **2022**, *16*, 165506. [CrossRef]
3. Yohan, A.; Lo, N.W. FOTB: A secure Blockchain-based firmware update framework for IoT environment. *Int. J. Inf. Secur.* **2020**, *19*, 257–278. [CrossRef]
4. Gandhi, G.M.; Salvi. Artificial intelligence integrated Blockchain for training autonomous cars. In Proceedings of the 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 14–15 March 2019; Volume 1, pp. 157–161.
5. Zhang, X.; Fan, M. Blockchain-based secure equipment diagnosis mechanism of smart grid. *IEEE Access* **2018**, *6*, 66165–66177. [CrossRef]
6. Al-Saif, N.; Ahmad, R.W.; Salah, K.; Yaqoob, I.; Jayaraman, R.; Omar, M. Blockchain for Electric Vehicles Energy Trading: Requirements, Opportunities, and Challenges. *IEEE Access* **2021**, *9*, 156947–156961. [CrossRef]
7. Zavolokina, L.; Miscione, G.; Schwabe, G. Buyers of 'lemons': How can a Blockchain platform address buyers' needs in the market for 'lemons'? *Electron. Mark.* **2020**, *30*, 227–239. [CrossRef]
8. Yang, Y.T.; Chou, L.D.; Tseng, C.W.; Tseng, F.H.; Liu, C.C. Blockchain-based traffic event validation and trust verification for VANETs. *IEEE Access* **2019**, *7*, 30868–30877. [CrossRef]
9. Misra, S.; Tyagi, A.K. *Blockchain Applications in the Smart Era*; Springer: Berlin/Heidelberg, Germany, 2022.
10. Ren, D. Application of Blockchain Technology in Practical International Technology Trade. In *International Conference on Cognitive Based Information Processing and Applications (CIPA 2021)*; Springer: Berlin/Heidelberg, Germany, 2022; Volume 2, pp. 687–694.
11. Huo, R.; Zeng, S.; Wang, Z.; Shang, J.; Chen, W.; Huang, T.; Wang, S.; Yu, F.R.; Liu, Y. A comprehensive survey on Blockchain in industrial internet of things: Motivations, research progresses, and future challenges. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 88–122. [CrossRef]
12. Mollah, M.B.; Zhao, J.; Niyato, D.; Guan, Y.L.; Yuen, C.; Sun, S.; Lam, K.Y.; Koh, L.H. Blockchain for the internet of vehicles towards intelligent transportation systems: A survey. *IEEE Internet Things J.* **2020**, *8*, 4157–4185. [CrossRef]
13. Krichen, M.; Ammi, M.; Mihoub, A.; Almutiq, M. Blockchain for modern applications: A survey. *Sensors* **2022**, *22*, 5274. [CrossRef] [PubMed]
14. Jabbar, R.; Dhib, E.; ben Said, A.; Krichen, M.; Fetais, N.; Zaidan, E.; Barkaoui, K. Blockchain technology for intelligent transportation systems: A systematic literature review. *IEEE Access* **2022**, *18*, 20995–21031. [CrossRef]
15. Aggarwal, S.; Kumar, N. Cryptographic consensus mechanisms. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2021; Volume 121, pp. 211–226.
16. Jansen, B.J.; Liang, H.; Ye, J. *International Conference on Cognitive Based Information Processing and Applications (CIPA 2021): Volume 2*; Springer Nature : Singapore, 2021; Volume 85.
17. Alam, T. Blockchain cities: The futuristic cities driven by Blockchain, big data and internet of things. *GeoJournal* **2022**, *87*, 5383–5412. [CrossRef]
18. Kapassa, E.; Themistocleous, M.; Christodoulou, K.; Iosif, E. Blockchain application in internet of vehicles: Challenges, contributions and current limitations. *Future Internet* **2021**, *13*, 313. [CrossRef]
19. Jaatun, M.G.; Haro, P.H.; Frøystad, C. Five things you should not use Blockchain for. In Proceedings of the 2020 IEEE Cloud Summit, Harrisburg, PA, USA, 21–22 October 2020; pp. 167–169.
20. Liu, H.; Zhang, Y.; Yang, T. Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Netw.* **2018**, *32*, 78–83. [CrossRef]
21. Bazel, M.A.; Mohammed, F.; Ahmed, M. Blockchain technology in healthcare big data management: Benefits, applications and challenges. In Proceedings of the 2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA), Sana'a, Yemen, 10–12 October 2021; pp. 1–8.
22. Wang, T.; Hua, H.; Wei, Z.; Cao, J. Challenges of Blockchain in new generation energy systems and future outlooks. *Int. J. Electr. Power Energy Syst.* **2022**, *135*, 107499. [CrossRef]
23. Abdel-Halim, I.T.; Fahmy, H.M.A. Mobility prediction in vehicular ad-hoc networks: Prediction aims, techniques, use cases, and research challenges. *IEEE Intell. Transp. Syst. Mag.* **2019**, *13*, 105–126. [CrossRef]
24. Zhang, R.; Wu, L.; Cao, S.; Xiong, N.N.; Li, J.; Wu, D.; Ma, C. MPTO-MT: A multi-period vehicular task offloading method in 5G HetNets. *J. Syst. Archit.* **2022**, *131*, 102712. [CrossRef]
25. Ji, B.; Chen, Z.; Mumtaz, S.; Han, C.; Li, C.; Wen, H.; Wang, D. A vision of IoV in 5G HetNets: Architecture, key technologies, applications, challenges, and trends. *IEEE Netw.* **2022**, *36*, 153–161. [CrossRef]
26. Wang, Y.; Zen, H.; Sabri, M.F.M.; Wang, X.; Kho, L.C. Towards Strengthening the Resilience of IoV Networks—A Trust Management Perspective. *Future Internet* **2022**, *14*, 202. [CrossRef]
27. Vishwakarma, L.; Nahar, A.; Das, D. Lbsv: Lightweight Blockchain security protocol for secure storage and communication in sdn-enabled iov. *IEEE Trans. Veh. Technol.* **2022**, *71*, 5983–5994. [CrossRef]
28. Kapassa, E.; Themistocleous, M. Blockchain technology applied in IoV demand response management: A systematic literature review. *Future Internet* **2022**, *14*, 136. [CrossRef]

29. Vrachkov, D.G.; Todorov, D.G. Automotive diagnostic trouble code (DTC) handling over the Internet. In Proceedings of the 2018 IX National Conference with International Participation (ELECTRONICA), Sofia, Bulgaria, 17–18 May 2018; pp. 1–3.
30. Chen, J.; Ruan, Y.; Guo, L.; Lu, H. BCVehis: A Blockchain-based service prototype of vehicle history tracking for used-car trades in China. *IEEE Access* **2020**, *8*, 214842–214851. [CrossRef]
31. Yoo, S.G.; Ahn, B. A study for efficiency improvement of used car trading based on a public Blockchain. *J. Supercomput.* **2021**, *77*, 10621–10635. [CrossRef]
32. Patro, P.K.; Ahmad, R.W.; Yaqoob, I.; Salah, K.; Jayaraman, R. Blockchain-based solution for product recall management in the automotive supply chain. *IEEE Access* **2021**, *9*, 167756–167775. [CrossRef]
33. Sharma, P.K.; Kumar, N.; Park, J.H. Blockchain-based distributed framework for automotive industry in a smart city. *IEEE Trans. Ind. Inform.* **2018**, *15*, 4197–4205. [CrossRef]
34. Chaudhary, B.; Singh, K. A Blockchain enabled location-privacy preserving scheme for vehicular ad-hoc networks. *Peer- Netw. Appl.* **2021**, *14*, 3198–3212. [CrossRef]
35. Lamssaggad, A.; Benamar, N.; Hafid, A.S.; Msahli, M. A survey on the current security landscape of intelligent transportation systems. *IEEE Access* **2021**, *9*, 9180–9208. [CrossRef]
36. Kulik, T.; Dongol, B.; Larsen, P.G.; Macedo, H.D.; Schneider, S.; Tran-Jørgensen, P.W.; Woodcock, J. A survey of practical formal methods for security. *Form. Asp. Comput.* **2022**, *34*, 1–39. [CrossRef]
37. Blanco, D.F.; Le Mouël, F.; Lin, T. Fenrir: Blockchain-Based Inter-Company App-Store for the Automotive Industry. *IEEE Access* **2022**, *10*, 122933–122953. [CrossRef]
38. Partovi, Z.; Zarei, M.; Rahmani, A.M. Data-centric approaches in the Internet of Vehicles: A systematic review on techniques, open issues, and future directions. *Int. J. Commun. Syst.* **2023**, *36*, e5383. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.