A Blockchain-Enabled IoT Framework for Vehicle Communication Using Ethereum

Anil Kumar Biswal[1*], Divya Midhunchakkaravarthy[2], Dharmesh Dhabliya[3]
[1,2]Lincoln University College, Malasiya
[1]Udayanath Autonomous College of Science and Technology, Cuttack, India
[3]Vishwakarma Institute of Information Technology, Pune, India
[1]anil.biswal123@gmail.com, [2]divya@lincoln.edu.my, [3]dharmeshdhabliya@gmail.com

Abstract: The idea of smart cities has become popular in big cities because of the rise of smart gadgets, systems, and technologies that are built in and connected. They have made it possible for every "thing" to connect to the Internet. The Internet of Vehicles (IoV) will be very important in the smart cities that will be built in the future as the Internet of Things becomes more common. The IoV could help fix a lot of traffic and road safety issues that could lead to deadly accidents. In the Internet of Vehicles (IoV), notably in Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) connections, it is important to make sure that data is sent quickly, safely, and accurately. This work involves using Blockchain technology for real-time application (RTA) to fix problems with Vehicle-to-Everything (V2X) connections in order to get around these problems. The primary innovation of this article is the development of a Blockchain-based IoT system aimed at facilitating secure communication and creating a fully decentralized cloud computing platform. Additionally, the authors qualitatively assessed the performance and resilience of the proposed system against prevalent security threats. Tests on computers indicated that the proposed approach fixed the key problems with Vehicle-to-X (V2X) communications, namely security, centralization, and a lack of privacy. It also made sure that different parts of intelligent transportation systems could easily share data with each other.

Keywords: Blockchain; Automotive Communication; Internet of Vehicles; Intelligent Transport System; Ethereum; Security.

1. Introduction

The Internet of Things (IoT) is a network of physical objects that have network connectivity, actuators, sensors, software, and electronics. Examples of these objects are household appliances, cars, and other things. The embedded computing systems identify each device and add it to the Internet infrastructure. Such gadgets can be controlled from afar thanks to the network architecture [1]. As a result, computer-based systems are becoming more and more connected to the real world. This is good for the economy, accuracy, and efficiency, and it means that people have to do less work. The technology is a type of cyber-physical system that includes smart cities, intelligent transportation, smart homes, virtual power plants, and smart grids. This is possible because of actuators and sensors.

The Internet of Things (IoT) is changing traditional vehicular ad-hoc networks (VANETs) into the Internet of Vehicles (IoV) [2]. The IoV is the real-time exchange of data between vehicles and between vehicles and infrastructure. This is done through smart terminal devices, vehicle navigation systems, mobile

communication technology, and information platforms that let people share driving instructions and control the network system.

This idea has made it easier to gather and share information about automobiles and infrastructure. It also lets you collect, compute, and share data with Internet systems and other information platforms.

This idea has recently become quite real. In the near future, 25 billion things are expected to be connected to the Internet, and cars will make up a large part of that [2]. Intelligent Transportation Systems (ITS) in Japan and Europe have already used some IoV technology. For example, 55,000 licensed rickshaws in New Delhi have GPS devices [3]. Because communication and processing technologies are developing so quickly, this idea has gotten a lot of attention from researchers and businesses. Also, smart cars are becoming more and more connected to the Internet, other cars nearby, and traffic management systems. This is how cars are becoming part of the Internet of Things (IoT). Still, this idea has several flaws, even though it offers clear benefits. It's very hard to keep smart cars safe since they are so connected, which makes them easy targets for bad people. Also, sharing sensitive data makes privacy problems worse. When it comes to smart cars, the usual ways of keeping things safe and private don't work. Here is a list of the primary problems:

• Centralization: Right now, smart vehicle architectures use centralized, brokered communication methods [4]. More specifically, central cloud servers find, verify, authorize, and connect all the cars. Still, it is not likely that this approach will be used on a larger scale. If cloud servers go down, the whole network might be in jeopardy.

• No Privacy: Most of the time, the current communication infrastructures don't protect users' privacy. To put it another way, information on the car is shared without the owner's permission. Also, the person who asked for the data gets noisy or summarized data.

• Heterogeneity: diverse groups, authorities, and people use connecting devices in IoV in very diverse ways. Also, their resolutions, functions, and ways of working are all different. So, it's hard to make sure that many gadgets can work together well at the same time. Combining these kinds of gadgets in a complicated network makes things much more complicated.

• Scalability: The utilization of small devices like sensors and actuators has been growing since embedded technologies are becoming more common. At the same time, the amount of data these kinds of gadgets make is expanding without end. So, another big problem with the IoV is keeping track of how many devices there are and the data they make.

• Interoperability: In the IoV ecosystem, both people and things that aren't people are actors.

In IoV applications, each actor can play different roles, such service provider, data consumer, data supplier, and available resource, depending on the environment and the scenario. For the IoV vision to come true, all the players need to be able to work together smoothly. If you handle each actor in a different way, their interactions get stronger.

• Mobility: The problems with mobility are connected to the efficiency of the protocol and the IoT network.

At present, sensor networks, Mobile Ad Hoc Networks (MANETs), and the mobility protocols of Vehicular Ad Hoc Networks (VANETs) are insufficiently equipped to manage conventional IoT devices due to significant processing and energy limitations. Also, instead of a one-time initial setup, real-time authentication is needed because the car needs to constantly authenticate other cars on the road.

• Threats to Safety: Smart cars are getting more and more features that let them drive themselves.

So, a security breach that happens because of a bug caused by installing malware might cause car wrecks and put other people on the road in danger.

VANETs are vulnerable to attacks like Man-In-The-Middle (MITM) attacks, which makes it exceedingly hard to keep them safe [5–7]. Malicious nodes (MITM) utilize these attacks to manipulate or listen in on messages sent between cars that include important or time-sensitive information, like a warning about a sharp curve. So, wrong and stolen information can spread all throughout the network. Also, Distributed Denial of Service (DDOS) can be used to stop people from using network services. In addition, DDOS in the context of connected vehicles can alter identities and spread false information, which can then cause a jam in the targeted network [8]. As a result, the key principles of security, which are integrity, confidentiality, and availability, are broken. In this case, Troy Hunt, a Microsoft Most Valuable Professional (MVP) in Security, was able to access car data and manipulate some vehicle systems from his home in Australia in February 2016 [9]. Then, in June 2016, a Mitsubishi Outlander PHEV [10] was hacked through its smartphone app for remote control, which let the user lock or unlock doors, change charger settings, and handle important non-driving things like air conditioning. Keen Security Lab, a Chinese cybersecurity company, has hacked Tesla [11]. This is not the first time Tesla has been hacked. Researchers [12] could also control the brakes, doors, and mirrors of a Tesla Model S from a distance of 20 miles (12 m). All of these events show how much we need a better way to communicate and send data that is safe, reliable, and fast. Blockchain [13,14] technology has recently demonstrated the capacity to enhance intelligent transport systems by rendering them secure, decentralized, and self-sufficient. This way, intelligent transport systems may use their infrastructure and resources, including crowd sourcing technologies, more efficiently. Blockchain is very important for solving the problems of privacy and security on IoV networks. To solve these problems, a Decentralized IoT Solution for Vehicles communication (DISV) based on the idea of Blockchain is suggested. More specifically, every member of the Internet of Vehicle networks gets messages and then sends them to a chosen Blockchain layer. The server will also check the received block against what it knows and decide whether or not to add it to the smart contract. The primary contributions of this study are threefold:

• A new IoT solution (DISV) to look at all the ways that smart city components and road users might interact with each other, such as automobiles, lights, radars, pedestrians, and more. This DISV has three main layers:

- The perception layer is made up of many Android apps (AV and AP) that are made to sense and gather information about drivers, vehicles, and infrastructure.
- The network layer, which lets devices and the cloud talk to each other over networks like 4G or wifi.
- The application layer, which is made up of cloud solutions that handle management, data analysis, and user services.

• A decentralized framework built on blockchain technology with a real-time application (RTA) specification that aims to make it possible for vehicles and other actors in transportation networks to talk to each other safely.

• The proposed system works well, especially when it comes to execution time, costs, availability, integrity, immutability, and security.

The rest of this paper is set up like this. An overview of Blockchain methods and Ethereum is given in Section 2. In Section 3, we look at how Blockchain can be used for the Internet of Things and, in practice, for the Internet of Vehicles. Section 4 goes into detail on the proposed system's design, including its parts

and essential steps. Section 5 talks about the findings of the computer tests that were done to see if the suggested system works and is reliable. Section 6 presents a summary of the key conclusion and suggests new areas for future investigation.

2. Blockchain Technique and Ethereum

Satoshi Nakamoto introduced Bitcoin in 2008, It is a decentralized global money cryptosystem that uses Blockchain technology [15]. Blockchain is used in Bitcoin to make sure that digital money may be safely exchanged for goods and services without a central authority. This is done through a trusted peer-to-peer network in a way that makes it look like the person is anonymous. Everyone on the network may see the blockchain or public ledger, which keeps track of all transactions. To be more specific, everyone has an exact copy of the Blockchain. Each transaction is put into a block, which is then time-stamped and made public. After that, transactions can't be changed or undone because the hash of the prior blocks is included in the next block's successors in each block of the chain. So, everyone agrees on the history of the transactions. Blockchain, which is a distributed ledger technology or, more accurately, a distributed database of records, has become quite popular because it worked successfully with bitcoin. It is now used in many different areas, not only finance. It has mostly become a dependable infrastructure for building platforms that offer different solutions. Blockchain technology is now the basis for platforms used in healthcare, transportation, payment processing and money transfers, supply networks, and more [16]. The most common use of Blockchain, though, is to make new cryptocurrencies that are better than Bitcoin when it comes to hashing algorithms and proof-of-work methods. The main goal of these changes is to speed up the process of verifying transactions. There are already 3,000 digital currencies since Bitcoin came out. The market cap is now thought to be $295 billion USD. Ethereum [17], Ripple [18], and Stellar [19] are other digital currencies that have become very popular. The Ethereum platform is being used for this study, and further information about it will be given in the next parts.

2.1. Ethereum

Ethereum is a Blockchain-based distributed computing platform that Vitalik Buterin [20] created in 2013 and released in 2015 after a successful online crowd sale. Also, Ethereum can execute the code of decentralized applications, making it a programmable Blockchain that users can utilise to build new applications. In particular, a piece of code known as a smart contract facilitates the transfer of value, information, and media via the creation, distribution, and management of blockchain-based decentralized software applications.

2.1.1. Ethereum Virtual Machine (EVM)

The Ethereum Virtual Machine (EVM) is a Turing-complete piece of software that greatly simplifies the development of Blockchain applications and allows users to deploy and run programs in various languages (such as Solidity). It is separate from the main network because it is a sandbox environment. And therefore, following the identical set of instructions, every Ethereum network runs its own EVM implementation. Ethereum tokens, or ETH, are used to fund EVM computations.

2.1.2. Transactions

Messages transmitted between two Ethereum accounts (the one sending the transaction and the one receiving it) constitute a transaction, which is a signed data package. The mining process, or more specifically, the generation of a signature by the owner of a transaction's private key, verifies the

transactions. There is mandatory data such as the Ethereum recipient address and optional data such as the petrol price (ETH gas Price), the maximum amount of petrol to be utilized, and the transferred amount.

2.1.3. Ether and Gas

For storage, processing, and contract code execution triggered by a message or transaction, the sender of the transaction must pay the Ethereum currency, Ether, which is in a state of constant volatility. In addition, gas is used to express the execution cost or the cost of using the network. Specifically, gas is a constant quantity that represents the amount of work that minors must put into computing in order to complete a specific operation. Customers pay for the gas required for the execution using Ethereum, therefore. As nodes in the Ethereum network, miners are responsible for receiving, propagating, verifying, and executing transactions. The gas limit specifies the most quantity of gas that the sender is willing to spend for transactions, taking into consideration that various operations have variable gas requirements. You can find more information on Ether and Gas in [21].

2.1.4. Proof-of-Work (PoW)

Evidence of- The work here is the original consensus algorithm that Blockchain relies on to verify the legitimacy of transactions. In PoW, users use specialized software to solve mathematical problems. Thus, Ethereum is updated whenever a new block of transactions is created by miners and added to the network by connecting it to the previous block. Each subsequent block incorporates the hash of the previous one. This means that the newly added block may now be followed all the way back to the first block, also known as the genesis block, in the chain.

3. Literature Review

Blockchain technology in nearly every aspect of the Internet of Things. The Internet of Things (IoT) makes it possible to connect healthcare practitioners, patients, and their families and friends in order to provide E-healthcare systems with clinical data. Electronic medical records (EMRs) are the primary means by which healthcare practitioners keep patient information. When compared to EMRs, the mobility of patient data in EHRs is far better. Using the idea of a distributed online database, Esposito et al. [22] developed a Blockchain-based plan for healthcare IoT applications. So, to investigate, examine records, and protect integrity, Liang et al. [23] used the Blockchain network in Android healthcare applications. 5G will improve the Internet of Things (IoT) in the telecommunications industry by connecting billions of items, allowing for a fully mobile society [24]. Privacy protection, however, will be an issue in the 5G heterogeneous communication environment. In order to address this concern, Fan et al. [25] devised a Blockchain-based plan to facilitate data exchange while guaranteeing user privacy.

The Internet of Things (IoT) refers to the network of interconnected computing devices that collect and transmit data via the Internet to a central server in the cloud using virtualization technologies. A blockchain-based intelligent resource management system for cloud data centres was created by Xu et al. [26]. A new trend with numerous potential applications has emerged in this area of study: the Internet of Vehicles (IoV). The foundation of this system is the Internet of Things (IoT), which facilitates intelligent communication between vehicles and other networks, including those connecting sensors, humans, roads, and other vehicles. The centralization of the security concept is lacking in numerous applications. Because of this, an ecosystem model based on Blockchain technology for managing charging piles and electric vehicles was created by Huang et al. [27]. To calculate the hash functions of electric vehicle charging heaps, this model uses Elliptic Curve Cryptography (ECC). Additionally, PETCON, a P2P electricity-

trading system, was created by Kang et al. [28] to demonstrate both the localized and comprehensive aspects of P2P electricity trading. It is not required to have a trustworthy authority for the PETCON system to use a consortium Blockchain approach to examine, validate, and publicly disseminate transaction records. Furthermore, Li et al. [29] developed CreditCoin, a privacy-preserving mechanism, to guarantee the proper forwarding of notifications without disclosing users' identities. Using an aggregation protocol, this system allows automobiles to transmit each other anonymous announcements using the Blockchain. Hence, trust in the exchange of IoV data is strengthened. As a last step, Yang et al. [30] suggested a reputation system that uses Blockchain technology to determine the reliability of data in the IoV. This system determines the veracity of the received messages based on the reputation values of the senders. When it comes to Intelligent Transportation Systems (ITS), Yong, Yuan, et al. [14] came up with a Blockchain approach to address security issues and performance limits. Authors included both required and optional car data, including insurance, taxes, and traffic rules, along with other useful data, such as weather predictions and traffic conditions.

Connecting VANET services and utilizing Blockchain's various functions, such as peer-to-peer communication, without compromising security or revealing personal information is the primary objective. Vehicles that do not require administration from a central manager can take advantage of the communication systems developed by Lei et al. [31] through dynamic key management using Blockchain. No other authority is needed because it relies on a decentralized Blockchain system. Key transfers are thus authentication and verification processes that the security manager network oversees.

To ensure that users' personal information remains secret, Dorri et al. [4] developed a Blockchain technology mechanism. At the same time, it revises the software for wireless remote controls and any other new services for automobiles (such as insurance, car sharing, smart charging, and electric vehicles). Because all models that try to improve the system's security and quality need extra communication protocols, latency is a problem in the IoV field. This is especially true when providing real-time cloud services to subscribers in the vehicular cloud. With fog computing, cloud users in vehicles can receive real-time services with little latency [32]. Connecting edge Networked Fog Centres (NetFCs) to vehicular clouds via single-hop mobile networks (i.e. I2V TCP/IP-based) was the suggested approach. This results in maximum efficiency and minimum time for vehicle service delivery. An adaptive resource management controller for new non-safety services between vehicles and infrastructure was created by the authors of [33]. Offloading traffic to local or remote clouds in vehicle-to-infrastructure applications was their main focus. Applications like these require QoS since they download and upload massive volumes of data. The results show that the controller is hard reliable for cloud service providers on a per-slot basis. Aloqaily et al.'s creative method [34] ensures ongoing vehicular services in smart cities by incorporating the notion of Smart Vehicle as a Service (SVaaS). Using a location prediction method, the solution is able to detect the vehicle's future location. This system uses a Quality of Experience (QoE) based service selection process to choose the necessary services before a vehicle reaches its destination once its expected position has been determined.

The idea of service availability was expanded upon by Al Ridhawi et al. in [35] to include a variety of cloud services for vehicles. Users and providers of cloud services were able to get these services by exchanging material. To find and select the service in both regional and international cloud service areas, state-of-the-art cloud negotiating entities and future location prediction models were employed.

The significance of "vehicle-to-everything" connectivity in smart cities prompted the development and testing of a new Internet of Things (IoT) Blockchain-based solution to improve and protect these conversations. Secure communications and fully decentralized cloud computing for the IoV can be achieved with the suggested system. Additional information regarding the suggested remedy is provided in the section that follows.

Table 1 compares and contrasts the current literature on the Blockchain solution for vehicle communication with the proposed work, demonstrating how numerous researchers and industry stakeholders have concentrated on developing intelligent communication concepts related to vehicle-to-vehicle (V2V) communications, such as smart cities, electric vehicles, Blockchain-based automotive communications approaches, Intelligent Transportation Systems, etc. First, in order to guarantee safe and rapid vehicular communication, M. Singh et al. [36–38] suggested a new Intelligent Vehicle-Trust Point (IV-TP), which helps to strengthen the security of vehicle-to-vehicle data sharing. This method is a smart data transfer system that utilizes blockchain technology, smart linked automobiles, and cloud computing for vehicles. Every smart vehicle may be identified during a communication session thanks to the unique identifiers assigned to them by IV-TP. One major benefit of IV-TP is the assurance it provides regarding the reliability of the vehicle in question. In addition, a distributed data management system for VECONs based on the consortium blockchain was suggested by J. Kang et al. [39]. Smart contracts allow Roadside Units (RSUs) to securely store and validate data, as well as keep track of data sharing history. Beyond that, they while designing a reputation-sharing data system, keep in mind the timing of occurrences, the similarity of paths, and the frequency of interactions. But there are limitations and security holes in the core design of conventional VANETs. B. Leidin et al. [40] suggested an Ethereum-based automated system for distributed vehicular network management, communication, and organization to circumvent these constraints. Also, in order to guarantee communication integrity among smart cities and associated IoT devices, E. Reilly et al. [41] established a novel light client protocol. To guarantee the trustworthiness of a transaction session, the authors' new approach included an obligatory authentication phase of data provenance that ran on an Ethereum address. Furthermore, compared to the NeuroMesh protocol, which is based on Bitcoin, the transaction costs through the suggested protocol are cheaper. Nevertheless, there are a few restrictions that make this application unusable in some situations. Actually, not all gadgets are compatible with operating systems. The solution also has limitations when it comes to time-sensitive applications, such as transactions, which can experience delays. There is a heightened vulnerability to hostile interventions or attacks in modern vehicle automotive systems.

G. Falco et al. [42] developed a framework for vehicles that verifies data sources and ensures the integrity, immutability, and reliability of shared information in order to make this step safer. Network scalability is guaranteed by the suggested method, which makes optimum use of the limited computational and networking resources of vehicles. In order to verify data changes such software updates, car identification, and distance driven, a consensus voting method based on DHTs is used. Another use of blockchain technology is the secure sharing of data.

S. Rowan et al. [43] established V2V communication as a robust and secure method of data transmission by utilizing both physical ultrasonic audio and visual light channels. In order to begin communication, a verification process is carried out to determine the ID and the location of the vehicle. The correspondent ID is accepted for future data exchange once it has been confirmed. Based on a public key Blockchain architecture and utilizing physical channels, the authors also suggested a new protocol for key production

that is utilized in inter-exchange vehicle sessions. Previous works had many restrictions, such as support for Turing completeness, which should be mentioned.

To be more precise, the majority of the aforementioned efforts employ Bitcoin as a means of implementing the Blockchain. However, due to its primary use as a cryptocurrency for safe, pseudo-anonymous commodity transactions, Bitcoin does not support smart contracts and does not come with programming features to solve computation problems, making it impossible to transfer various types of sensitive information. Blockchain platforms that enable Turing-complete operations, like Ethereum, are essential for the development of state-of-the-art vehicle communication systems. Since Blockchain relies on mining processing, earlier efforts also omitted performance calculations, specifically execution time. If you want to share data on the Blockchain, you'll need to mine it first. The mining process could take as long as ten minutes [44]. How long it takes is dependent on the specific data, smart contract type, and underlying technology. This means it might not be able to provide real-time warnings, as when a driver could be involved in an accident.

The time-consuming mining procedure limits the efficacy of any suggested Blockchain for vehicular communication. This study proposes a Decentralized Internet of Things (IoT) Solution for Vehicles Communication (DISV) built on the Ethereum platform. It is based on the Blockchain concept and has a real-time component that supports Turing-Completeness. The designed solution's real-time component is proven by the performance test.

4. Proposed Solution

4.1 System Overview

The goal of this paper is to show how an IoV solution with Real-Time Application (RTA) works. This approach makes it safe for vehicles to talk to each other and to other people in transportation systems. It tries to get around problems like execution time, which makes performance better. We made a prototype of DISV and tested it by sending a message over Blockchain to the nearest automobiles if a driver is sleepy. The proposed solution should have three primary layers: the perception layer, the network layer, and the application layer. This is because it is based on an IoT design. These layers and explains them below:

1. The physical layer is the perception layer. It is made up of a number of IoT devices that have sensors that can find and gather information about the environment (i.e., physical parameters) and smart objects that are close by. The Android Application for Vehicles (AV) that is part of the perception layer gathers and analyses information about the trip, the car, and how the driver acts. The Android Application for Infrastructure (AP) acts like IoT devices that are built into roadways, like radars, traffic lights, electronic signs on the side of the road, and more.
2. The network layer connects the sensors to other servers, network devices, and smart things. It also sends and interprets data from the sensors.
3. The application layer is made up of the Blockchain application and the Central Cloud Server. It gives IoT devices services that are customized to their applications. The Blockchain application, to be more specific, controls how vehicles and other people in the transportation system talk to each other. The Central Cloud Server is in charge of processing and analyzing the data it gets and sending out invites to other people.

Figure 1 shows the architecture of the proposed system and the basic process, which has three key components. The first step is for the automobiles to send data to the central server (1). Second, the central server sends an invitation to join to the Blockchain layer (2) depending on the information it got. Third, the autos may safely share data with other IoV participants in the same region (3).

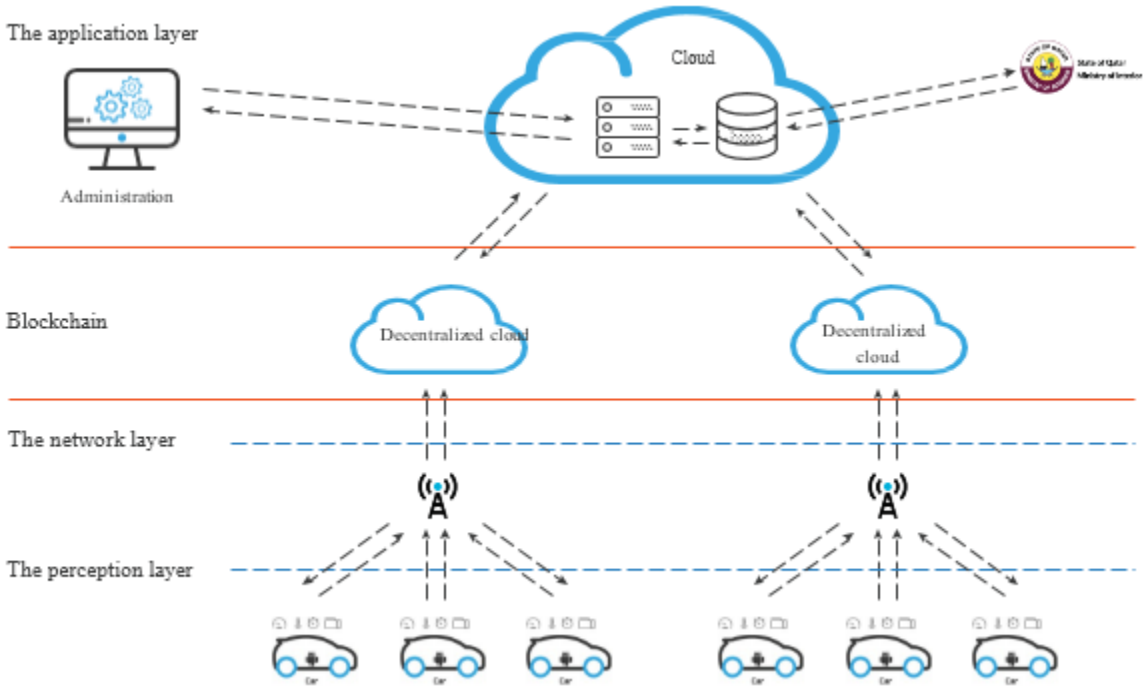

Figure 1. The architecture of the proposed Internet of Things solution.

A. The Perception Layer

To test different situations with different parts, an Android app has been made for vehicles (AV) and for infrastructure (AP), as explained in the next sections.

B. Android Application for Vehicles (AV)

AV is an Android app that has two parts. The Vehicle Data Collection System (VDCS) is the first subsystem. It gathers information on the trip and the car. The second system is called the Driver Drowsiness Detection system. It gathers information about the driver's behavior to see if they are sleepy or not.

The purpose of VDCS is to gather information about the car, like the model and the motor's horsepower, speed, and size. Finally, as shown in Figure 2, the system gathers information about the trip, such as the start and end times, the distance travelled, and the minimum, maximum, and average speeds. It is programmed to check for things like rotational velocity along the Roll, Pitch, and Yaw axes, acceleration, distance, and GPS position every 15 seconds.

The goal of Driver Drowsiness Detection is to find out if a driver is sleepy and stop any accidents that might happen as a result. This system is part of the Advanced Driver Assistance System (ADAS), which is a key feature of modern car technology. ADAS's job is to make driving safer and more enjoyable. This system was made utilizing Deep Neural Networks techniques to detect whether a driver is drowsy in real time. You may get more information about this system in [45–47].

The Android app features four main pages. You can log in on the first page with your username and password. After the user logs in, they can either start a new journey or get details about the last five travels on the second page. If the user picks a new journey, the app will start recording and showing all

the information as indicated in the last section. Then, it will use the web service to deliver the data it has gathered to the cloud server. The front camera will take a picture of the driver's face and show it on the fourth page.

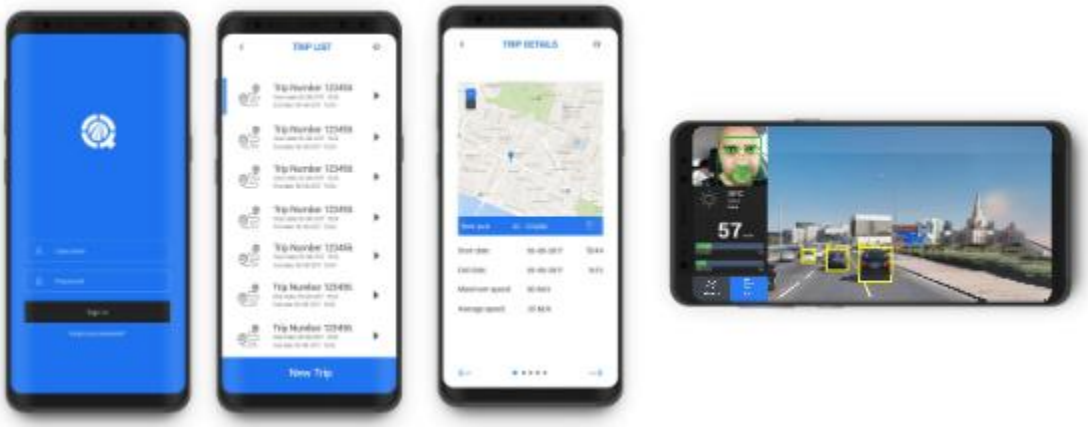

Figure 2. Screenshot of the four main pages of the Android application for Vehicles (AV).

Android Application for Infrastructure (AP)

The aim of this application is to simulate the role of IoT devices integrated into the roads such as radars, traffic lights, roadside electronic signs and others.

Many additional options of the Android application, such as traffic jams, the speed of cars, and weather conditions can be added to the perception layer.

The Network Layer

The network layer establishes the connection between the servers and transmits, and processes the sensor data. The application can use either Wi-Fi or mobile internet (3G/3G+/4G) to send the data to the server.

This collection process uses the hybrid system to gather and store data locally before transmitting it them to the server. This technique is proven to be highly effective for data collection when the Internet connection is poor or unstable.

C. The Application Layer

Regarding the application layer, it contains two principal compounds: Central cloud server and the communication system using a Blockchain Network.

i. Central Cloud Server

The central cloud gives the end user services that are customized to their application. It delivers the data it has gathered to the web services for processing and analysis before showing them to the end user. The web service is a part of the application layer that lets different parts of the IoT solution, like the website, database server, IoT devices, and embedded systems, talk to each other. Microsoft's Windows Communication Foundation is what makes the web service work. It uses the REST Architecture and JSON message format. It also gets information regarding crashes from the General Directorate of Traffic at the Ministry of Interior, as well as road conditions or any other information from other authorities that might be useful. The website gives the end user direct access to the web services, which makes the data available to them.

The researchers utilize the web application as a way to talk to and ask questions about the data that has been recorded. The website content in Figure 3 shows demographic information about the driver, such

as their nationality, gender, and age. It also has details about the car, like the model and when it was put into service.

Figure 3. Screenshot of a real trip displaying information about the vehicle and the driver.

By using Google Maps, the website displays the tracked trip and the position of individual events, as well as the details of all recorded events as shown in Figures 4 and 5.

Figure 4. Screenshot of a real trip displaying the data recorded for every event.

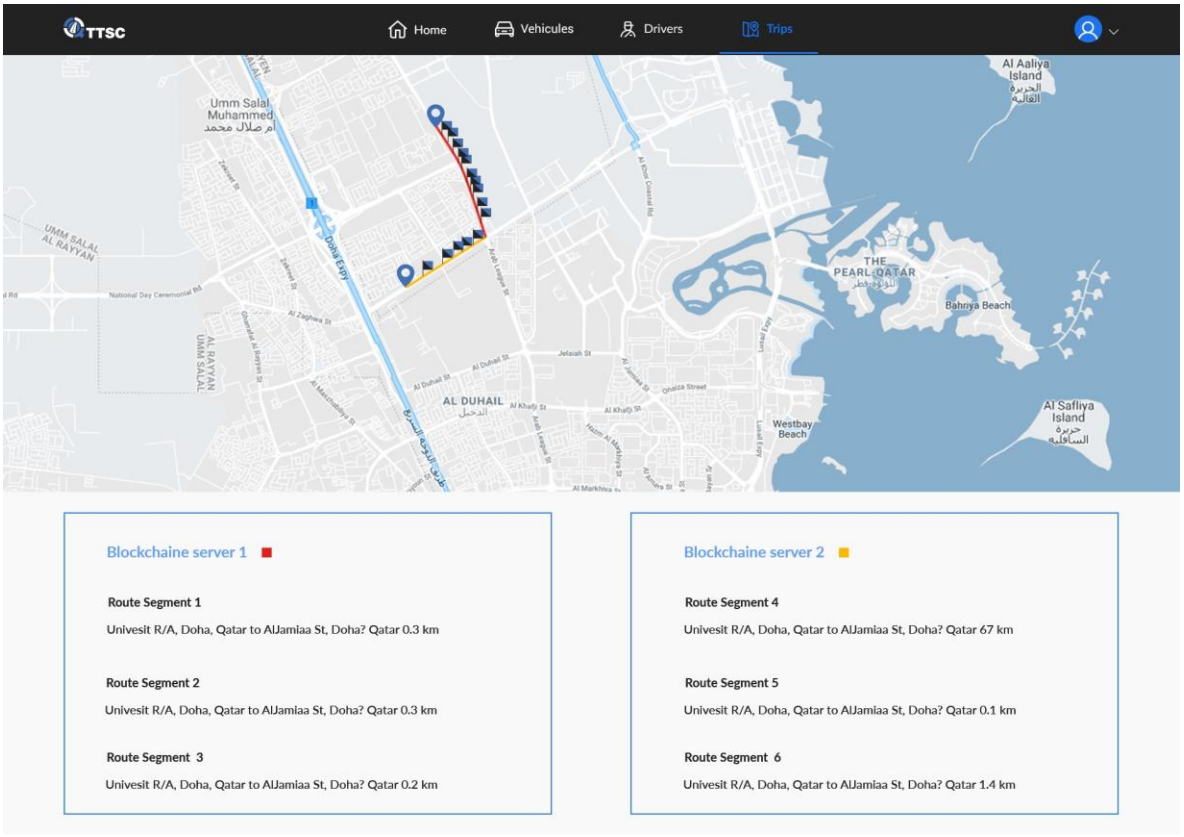

Figure 5. Screenshot of a real trip displaying the Blockchain layer for every road section.

4.2 The Blockchain Layer Blockchain Layer Overview

The Blockchain layer is what lets cars talk to each other. Every time slot, the car sends the data it has gathered to the central server using a web service. The information tells you where the user is right now and if they are connected to one of the Blockchain layers that are already there. After that, the primary server tells local IoT devices to connect to an open Blockchain cloud. The contact starts after the person accepts the invitation. Figure 6 demonstrates that each road section has a Blockchain layer that sends messages to the associated IoT devices.

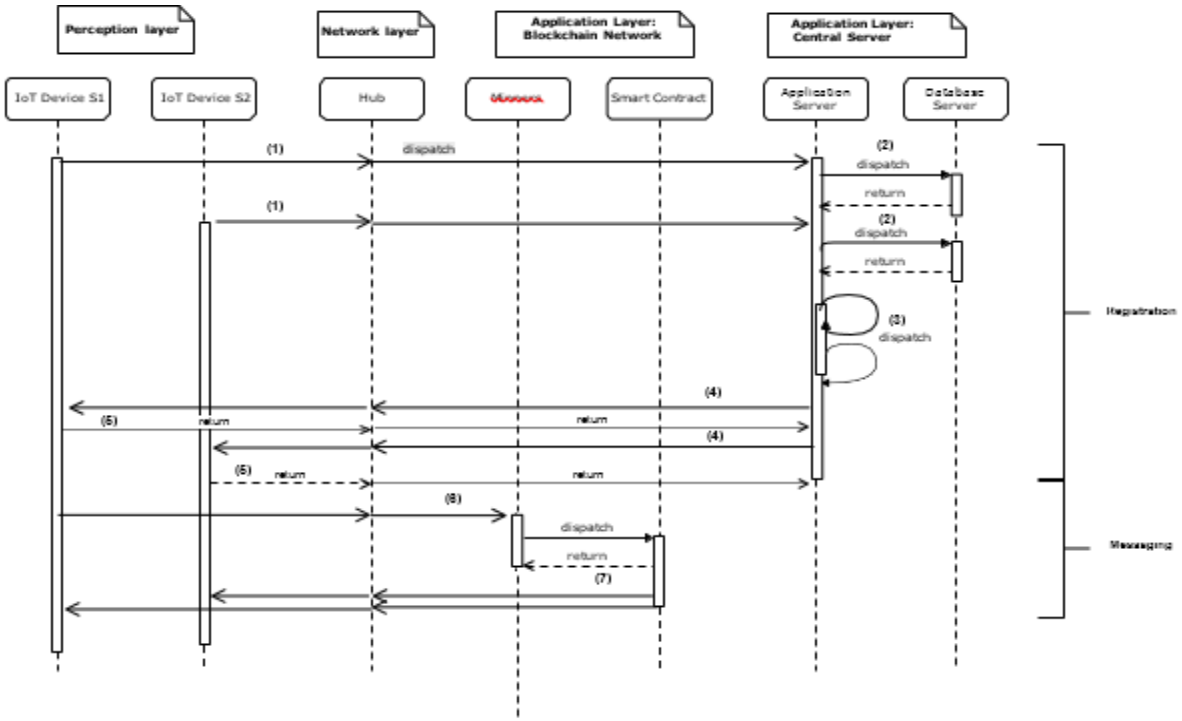

Figure 6. Sequence diagram of nominal scenario of communication between Internet of things (IoT) devices.

4.2.1 System In- Depth

The Android app and the Blockchain layer work together to make decentralized apps (Dapp, dApp, or DApp). In more detail, decentralized applications are Internet apps that run on a decentralised P2P network (Blockchain). Their code is open source, which means that anyone may see it and change it. As seen in Figure 7, dapp apps do not need a central server like regular apps do.

The Blockchain layer is the back end of the decentralized apps, and the Android app is the front end. In order to transmit a message over the Blockchain network, the mobile app calls functions of the smart contract that is running on each Ethereum node. The communication goes through a wrapper that connects the mobile and node-endpoint. This research used one of the most dependable frameworks: The Web3.Js for Android framework. Its smart contract serves two main purposes. The first function, setMessage, is in charge of putting a new message on the Blockchain network for the amount of ETH that the sender is ready to pay for each unit of gas needed to mine the message. The second function, GetMessage, lets the device that is connected to the Blockchain network read the data that is already there.

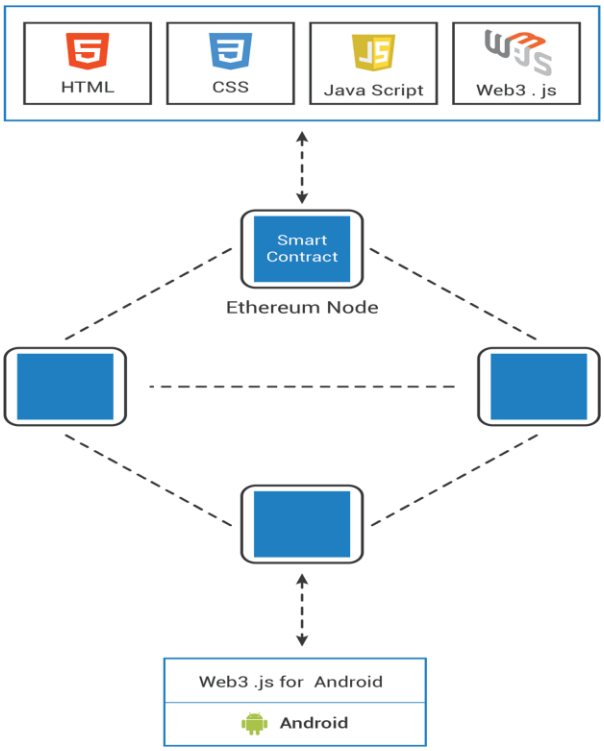

Figure 7. The architecture of decentralized applications (Dapp).

There are some restrictions on how Blockchain can be used to connect automobiles with other people in the transportation sector. The biggest worry is how long it will take to add the transaction to a block chain. Because it takes time to update the smart contract, the DISV can't be called a real-time application. Because of this, a number of steps are suggested to cut down on the smart contract's content and, as a result, the time it takes to complete. First, instead of having one Blockchain layer handle communication in a vast area, having various Blockchain layers in smaller areas would make it easier for a limited number of cars to talk to each other. Second, all messages should be deleted from the system after the competition is over. When the communication is no longer needed, the smart contract deletes it after the central data gets a copy.

4.2.2 Nominal Scenario

This part talks about the normal way that IoT devices talk to each other. The sequence diagram in Figure 6 demonstrates that the normal scenario is split into two parts: registration and messaging. During the registration process, the IoT device sends the data it has collected to the central server over the Internet (1) every 15 seconds. The database server (2) stores the data that the central server collects. The server also looks for IoT devices that are close by, such traffic signals, roundabouts, or other areas (3). Next, an invitation is made to the devices in the same place to talk to each other via one of the Blockchain layers (4). The second sub-process starts after the invitation is accepted.

The IoT devices are now linked to one other and can send data to each other in the messaging stage. The Blockchain network is used by the IoT devices to convey the message. After the mining process (6), the message is uploaded to the smart contract so that all the devices linked to this server Blockchain layer can get it (7).

5. Evaluation and Discussion of Performance

We can use numerous methods to figure out how well a software solution works [49,50]. It is especially important to look at the precise features that the solution needs to work well. Figure 8 shows that the primary features of the proposed system are execution time, costs, availability, integrity, immutability, and security. In order for the solution to work perfectly, all of these properties must work at their best. This study will examine these aspects to evaluate the overall efficacy of the solution.

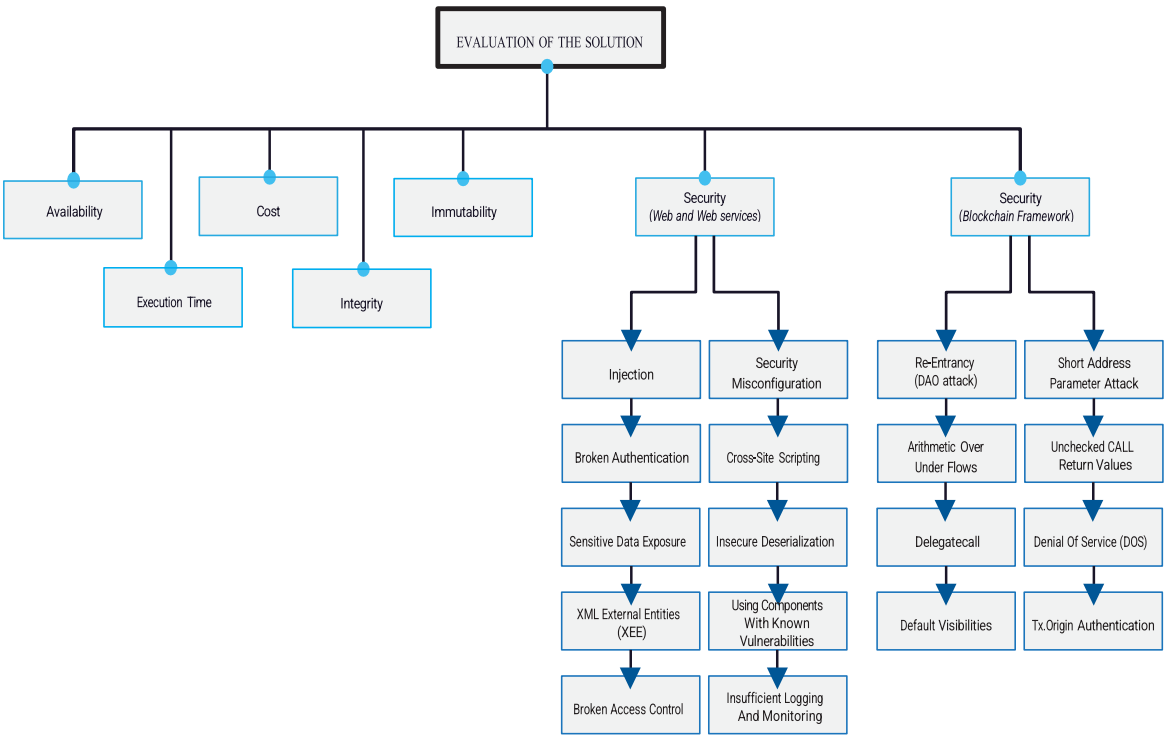

Figure 8. System evaluation diagram.

5.1 Costs

The Ethereum network's Testnet was utilized to put the smart contract prototype into action. This part looks at the costs of making and carrying out the smart contract. The following values were used, which were true in January 2020: 1 gas_1 wei (0.000000001 ETH) = 1 ETH $161.92 US. At the time of the investigation, the average gas value was about 0.006845 Ethereum, while the lowest gas value for a transaction was 1 wei.

1 Gas = 0.006845 Ethereum (ETH) Gas Price = 6,138,887 Gwei

The SetMessage method doesn't cost much; on average, it costs $0.03523 US. But the costs of "SetMessage" functions can be very different because the length of the message input can change. Still, one byte costs 136 petrol, which is around $0.00003 US. The GetMessage function, on the other hand, doesn't cost anything extra because you don't have to mine anything to get messages from the blocks and the smart contract doesn't need any updates.

5.2 Execution Time

Execution time is one of the most important things to look at when judging transport management systems like DISV. In fact, even a small delay in sending or receiving signals can cause big problems for

the system. To make sure that the blockchain-based communication framework between vehicles and all other parts of the transportation system works properly, it is important to add each message to the smart contract on time. This is because the mining process depends on solving complex problems.

Execution time is particularly crucial because the proposed prototype is a real-time application. In computational testing, the times it takes for each function of the Android app to run are measured. To test how well the proposed Ethereum private Blockchain solution worked, a server with 64 GB of RAM and a Core i7-000 was employed.

Figure 9 indicates that the GetMessage function's server responds much faster than the SetMessage function's server. When the server gets 1000 requests, it takes between 1 millisecond and roughly 10 milliseconds to call the GetMessage method. So, it doesn't matter if you call the GetMessage method once or a hundred times; the time it takes to run is about the same. But it takes a long time to invoke the SetMessage method because the message needs to be mined first so that it can be included to the smart contract. When the server gets ten requests to contact the SetMessage function, it takes 1.64 seconds. When it gets five hundred requests, it takes more than 90 seconds. The computational investigation indicated that, for various reasons, it is inadvisable for the list SetMessage to exceed 25 messages.

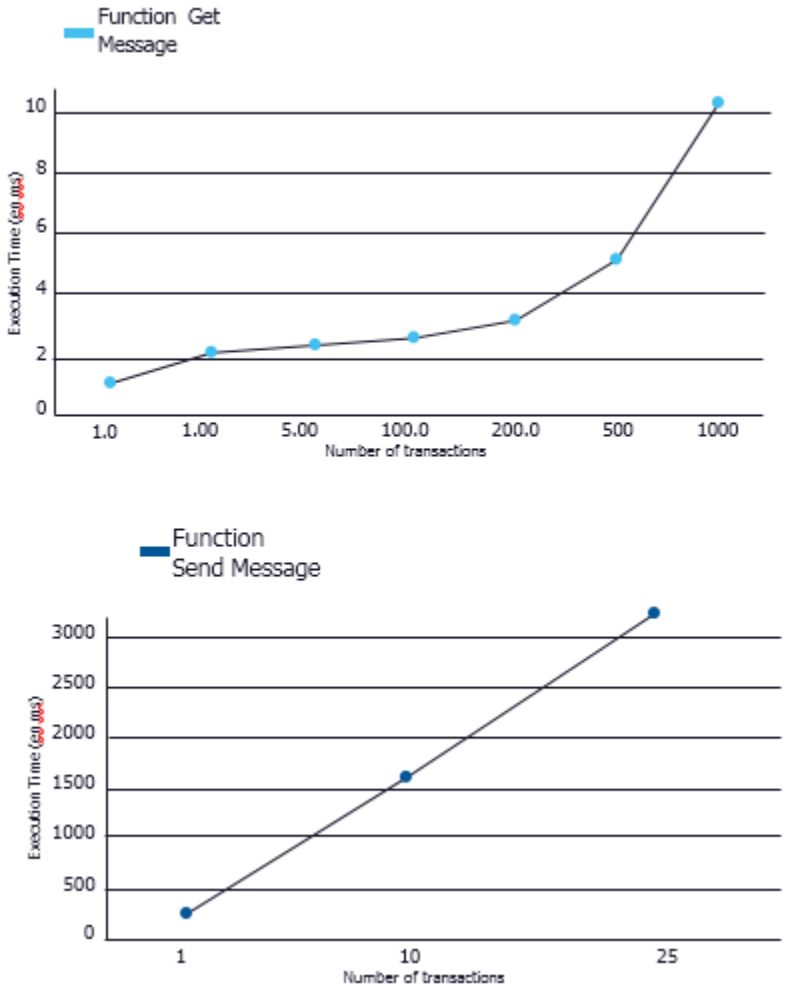

Figure 9. Execution time of the different functions in the Decentralized IoT solution for Vehicles communication (DISV) in milliseconds.

One of DISV's most important features is that it can conduct transactions in real time, which means that they should only take a short amount of time to complete. such, the proposed architecture suggested using the Blockchain layer in each zone such that the server only gets and sends a few messages.

The Android app uses numerous Blockchain layers and gets rid of old and duplicate communications so that the smart contract only has the messages it needs. If you use the suggested architecture, the messaging server in DISV usually responds in 0 to 3 seconds. Because of this, DISV might be called a real-time application (RTA).

5.3 Memory and Power Use

Since DISV employs Blockchain for the IoT, it is important to look at how much power and memory it uses, since IoT devices normally don't have much of either. The demo used a Huawei P8 Lite with 2 GB of RAM, a Li-Po 2500 mAh battery, and a Hisilicon Kirin 620 Processor for the calculations. Figure 10 shows that the Android solution we made uses a lot less memory than other commercial apps, like Facebook (134 MB), WhatsApp (106 MB), and Skype (233 MB). Figure 11 shows that the proposed solution uses an average of 23.43 mAh of electricity, which is about the same as Skype (21.66 mAh) and Facebook (18.56 mAh).

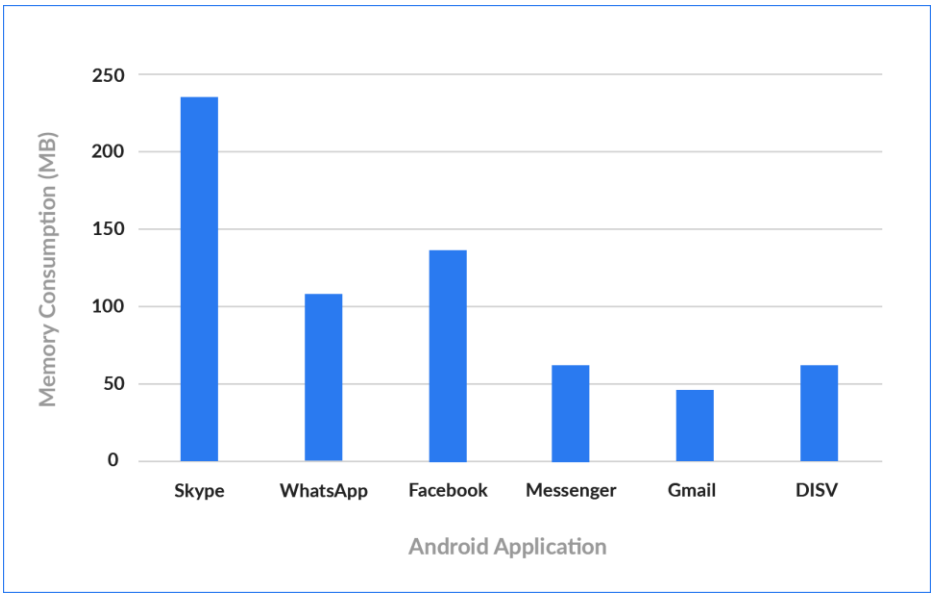

Figure 10. Comparing Memory Consumption of DISV with commercial mobile applications.

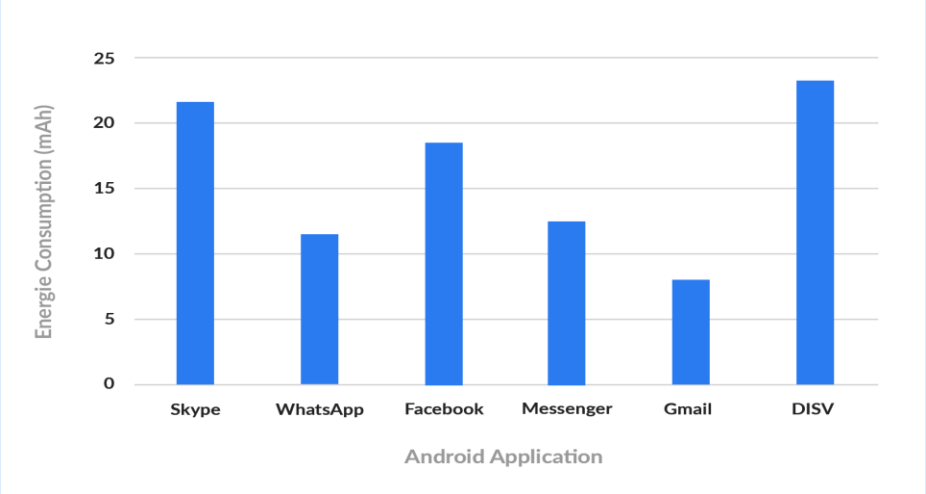

Figure 11. Comparing Energy Consumption of DISV with commercial mobile applications.

Availability

Another critical property of transportation management systems such as DISV is availability. More precisely, even the minor temporary shutdown of the system is likely to lead to traffic congestion and crashes. Availability means that a system is online and ready for access at any time. A variety of factors can cause a shutdown of the system (off-line), ranging from planned downtime for maintenance to sudden failure. The decentralized and robust nature of the Blockchain prevents attacks such as a denial-of-service (DoS) attack [51,52], which only target nodes [53], as the central party cannot be a single point of failure [52]. Yet, the distribution of the Blockchain is not complete. The mining power is typically limited to miners residing in approximately the same location. Thus, this enables isolating them by hijacking some border gateway protocol (BGP) prefixed with a routing attack employing the internet infrastructure [53]. Considering the comprehensiveness of the Internet, the Ethereum Blockchain network must be always reachable. Solutions that are centralized but whose databases redistributed are vulnerable to routing attacks because of potentially hindered communication with and between the physical databases. Thanks to the resiliency of the Blockchain malicious and damaged nodes on the network can be handled.

One of the greatest threats to the availability of a Blockchain solution is 51% attacks, which is the ability of someone controlling a majority of network hash rate to revise transaction history and prevent new transactions from confirming. As opposed to a public chain, these messages delays are combined with the heterogeneous power of miners in such a private chain could easily allow a 51% attack and lead to the Blockchain anomaly.

5.4 Integrity

Integrity is another fundamental property of the systems which exchange sensitive data among the users. Thus, it is necessary to assess the data integrity property of the proposed software solution. Data integrity refers to the accuracy and reliability of data through the whole life cycle. It is critically related to the concept of data security. Uncorrupted data is whole, and it remains unchanged in regard to its complete state. It is essential for ensuring security to keep data consistent throughout its life cycle. The reliability of data refers to compliance with the following standards:

The accuracy of data – free from errors and confirmed by the protocol.
The originality of data – accessible sources and preservation in the original form.
Contemporary – data must be recorded at the exact time it was executed and observed.
Legible – easy to understand, record permanently, and preserve original entries.
An attributable – clear demonstration of who observed and recorded data, at what time, and what it is about.
Cryptographic Hashing and Merkle Trees are in charge of keeping the integrity of the data on public and private Blockchains intact. There are three main advantages of Merkle trees. First, they ensure the validity and integrity of data. Second, their proofs are fast and computationally easy requiring less disk space or memory. Third, their management and proof needs minimal information to be transmitted across networks. Moreover, Cryptographic Hashing is critical for keeping the integrity and security of data recorded on Blockchain. Encryption guarantees security, whereas integrity is achieved by ensuring that signatures update when the data is changed. Therefore, considering that the DISV is based on blockchain technology, it ensures the communication between vehicles which maintains data integrity at all times.

5.5 Consistency

One of the major criteria for a new system evaluation is consistency which refers to the requirement that a series of measurements of the same project yields comparable results when different raters perform it by the same method. The proposed solution has employed the Ethereum Blockchain to build the consensus mechanism. Accordingly, as explained in, explicit reconciliation processes are not required. The consistency mechanism is based on the assumption that the branch behind the most Proof-of-Work represents the real branch. To ensure consistency, each block in the Blockchain accepted by a node preserves the consistency of the local replica of the database. In a case of a temporary disagreement among the nodes on the real consistent truths, Proof-of-Work enables the automatic resolving of the fork. Honest nodes cannot under any circumstances adapt to inconsistent chains. Within the network, the deeper buried blocks in the chain are always consistent. Considering Proof-of-Work prevents unsolvable reconciliation process, it is evident that the Blockchain ensures consistency in the proposed DISV system.

5.6 Confidentiality

In the context of computer systems, confidentiality means that only authorized users can see sensitive and protected data. So, it is important to include some features that will keep information private and protect it from bad people. In a Blockchain setup, confidentiality lets people involved in a transaction do it without letting other people know specific facts or details about it. Public blockchains like Bitcoin and Ethereum don't believe in privacy, thus all of their transactions are public. In contrast, private blockchains can keep transactions and the identities of the nodes that are involved private as long as they are protected. To meet these needs, the suggested solution must meet the following needs:

An unauthorized third party must be able to see who the other parties are in a Blockchain transaction unless the other parties tell them that information.

The individual who isn't part of a transaction shouldn't be able to see the details of that transaction unless the people who are part of it share their information.

5.7 Unchanging

Immutability means that changes can't be made once something has been made. To change a transaction from history, you have to re-mine all the blocks that come before the one you want to change. This will then show up in every copy of the ledger on the network. It would also mean recreating the Merkle tree

for the block that the transaction is in and executing all the proof of work for that block again. Also, since the next block holds the hash of this block, it needs to be re-mined. The updated "previous block hash" must be added to the next block, which changes the block hash. In some situations, a hash like this would not match the stated difficulty level, which means that the block would need to be mined again. The re-mining will have to happen all the way to the last block in the chain. While the miner is re-mining old blocks, new blocks will be added to the chain at the same time. This means that the miner will have to edit both the old blocks and the new blocks at the same time. This action is nearly impossible because it requires so much computational power. As a result, the suggested DISV system guarantees that things won't change.

5.8 Safety

We used the Open Online Application Security Project (OWASP) Foundation's list of the top online vulnerabilities to check the security of the DISV system's central server, websites, and web services. OWASP is a non-profit group that wants to give security professionals and developers useful and unbiased knowledge about application security. Its main focus is on the most serious security holes in online apps. The system now includes the suggested requirement. But every day, fresh and complicated attacks happen. So, following the advised steps to stop the assaults won't completely stop them, but they will make it less likely that the system will be damaged or hacked.

6. Conclusions and Future Work

This article presented an innovative Decentralized IoT system for vehicular communication (DISV). It has three main levels that look into the feasibility of using Blockchain for communication in the IoV. A prototype of the smart contract has been put on the Ethereum Testnet. This study examined many attributes of the solution, including availability, integrity, and security, to evaluate the Blockchain as an effective and secure framework for IoV communications. The findings indicated that DISV qualifies as a real-time application and addresses the primary issues of Vehicle-to-X (V2X) communications, including security, centralization, and insufficient privacy. It can also let cars, infrastructure, and other parts of intelligent transportation networks share data and work together. Also, DISV could be a key part of Advanced Driver Assistance Systems (ADAS) that could make transportation safer and easier. An improved version of DISV will be created as a guideline for future research.

References

1. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. Comput. Netw. 2010, 54, 2787–2805.
2. Yang, F.; Wang, S.; Li, J.; Liu, Z.; Sun, Q. The internet of things: A survey. China Commun. 2014, 11, 1–15.
3. Delhi: 18,000 Autos Install GPS in One Month, Deadline Extended to February 28. Available online: https://www.hindustantimes.com/delhi-news/delhi-18-000-autos-install-gps-in-one-month-deadline-extended-to-february-28/story-xlIsXOhh94aKOxaO5wwErJ.html (accessed on 18 November 2019).
4. Dorri, A.; Steger, M.; Kanhere, S.S.; Jurdak, R. BlockChain: A Distributed Solution to Automotive Security and Privacy. IEEE Commun. Mag. 2017, 55, 119–125.

5. Al-kahtani, M.. Survey on Security Attacks in Vehicular Ad hoc Networks (VANETs). In Proceedings of the the 6th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, Australia, 12–14 December 2012; Volume 12–14, pp. 1–9.
6. Ahmad, F.; Hall, J.; Adnane, A.; Franqueira, V.N.L.. Faith in Vehicles: A Set of Evaluation Criteria for Trust Management in Vehicular Ad-Hoc Network. In Proceedings of the the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Exeter, UK, 24–27 July 2017; Volume 21-23, pp. 44–52.
7. Aloqaily, M.; Otoum, S.; Al Ridhawi, I.; Jararweh, Y. An Intrusion Detection System for Connected Vehicles in Smart Cities. Ad Hoc Networks 2019, 90, 101842.
8. Glass, S.M.; Muthukkumarasamy, V.; Portmann, M. Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks. In Proceedings of the the International Conference on Advanced Information Networking and Applications, Bradford, UK, 26–29 May 2009; Volume 26–29, pp. 530–538.
9. Controlling Vehicle Features of Nissan LEAFs across the Globe via Vulnerable APIs. Available online: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/ (accessed on 15 January 2020).
10. Hackers Discovered It is Possible to Remotely Control Features of Mitsubishi Outlander PHEV by Hacking the Mobile Applications Designed by the Car Vendor. Available online: https://securityaffairs.co/ wordpress/48114/hacking/mitsubishi-outlander-phev-hacking.html (accessed on 15 January 2020).
11. Tesla Fixes Security Bugs After Claims of Model S Hack. Available online: https://www.reuters.com/article/us-tesla-cyber/tesla-fixes-security-bugs-after-claims-of-model-s-hack-idUSKCN11Q2SD (accessed on 15 January 2020).
12. Team of Hackers Take Remote Control of Tesla Model S from 12 Miles Away. Available online: https://www.theguardian.com/technology/2016/sep/20/tesla-model-s-chinese-hack-remote-control-brakes (accessed on 15 January 2020).
13. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City. JIPS 2017, 13, 184–195.
14. Yuan, Y.; Wang, F.Y. Towards blockchain-based intelligent transportation systems. In Proceedings of the IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil, 1–4 November 2016; pp. 2663–2668.
15. Bitcoin: A Peer-to-Peer Electronic Cash System. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 15 January 2020).
16. Cruz; P.J.; Kaji, Y.; Yanai, N. RBAC-SC: Role-Based Access Control Using Smart Contract. IEEE Access 2018, 6, 12240–12251.
17. Ethereum. Blockchain App Platform. Available online: https://ethereum.org/ (accessed on 15 January 2020).
18. Ripple.Available online: https://ripple.com/ (accessed on 15 January 2020).
19. Stellar. Available online: https://www.stellar.org/ (accessed on 15 January 2020).

20. Wood., G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Yellow Paper. Available online: https://ethereum.github.io/yellowpaper/paper.pdf (accessed on 15 January 2020).
21. Ethereum Homestead Documentation. Available online: https://ethereum-homestead.readthedocs.io/en/ latest/index.html (accessed on 15 January 2020).
22. Esposito, C.; Santis, A.D.; Tortora, G.; Chang, H.; Choo, K.K.R. Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? IEEE Cloud Comput. 2018. 5, 31–37.
23. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating Blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017.
24. Ferrag, M.A.; Maglaras, L.; Argyriou, A.; Kosmanos, D.; Janicke, H. Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. J. Netw. Comput. Appl. 2018, 101, 55–82.
25. Fan, K.; Ren, Y.; Wang, Y.; Li, H.; Yang, Y. Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. IET Commun. 2018, 12, 527–532.
26. Xu, C.; Wang, K.; Guo, M. Intelligent Resource Management in Blockchain-Based Cloud Datacenters.IEEE Cloud Comput. 2017, 4, 50–59.
27. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A security model for electric vehicle and charging pile management based on Blockchain ecosystem. IEEE Access 2018, 6, 13 565–13 574.
28. Kang, J.; Yu, R.; Huang, X.; Maharjan, S.; Zhang, Y.; Hossain, E. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. IEEE Trans. Ind. Informatics 2017, 13, 3154–3164.
29. Li, L.; Liu, J.; Cheng, L.; Qiu, S.; Wang, W.; Zhang, X.; Zhang, Z. CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network for Communications of Smart Vehicles. IEEE Trans. Intell. Transp. Syst. 2018, 19, 2204–2220.
30. Yang, Z.; Zheng, K.; Yang, K.; Leung, V.C.M. A blockchain-based reputation system for data credibility assessment in vehicular networks. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
31. Lei, A.; Cruickshank, H.; Cao, Y.; Asuquo, P.; Ogah, C.P.A.; Sun, Z. Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems. IEEE Internet Things 2017, 4, 1832–1843.
32. Shojafar, M.; Cordeschi, N.; Baccarelli, E. Energy-efficient adaptive resource management for real-time vehicular cloud services. IEEE Trans. Cloud Comput. 2016, 7, 196–209.
33. Cordeschi, N.; Amendola, D.; Shojafar, M.; Baccarelli, E. Distributed and adaptive resource management in cloud-assisted cognitive radio vehicular networks with hard reliability guarantees. Veh. Commun. 2015, 2, 1–12.
34. Aloqaily, M.; Al Ridhawi, I.; Kantraci, B.; Mouftah, H.T. Vehicle as a Resource for Continuous Service Availability in Smart Citites. In Proceedings of the IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017.

35. Al Ridhawi, I.; Aloqaily, M.; Kantarci, B.; Jararweh, Y.; Mouftah, H.T. A continuous diversified vehicular cloud service availability framework for smart cities. Comput. Networks 2018, 145, 207–218.
36. Singh, M.; Kim, S. Blockchain based intelligent vehicle data sharing framework. arXiv 2017, arXiv:1708.09721.
37. Singh, M.; Kim, S. Intelligent vehicle-trust point: Reward based intelligent vehicle communication using blockchain. arXiv 2017, arXiv:1707.07442.
38. Singh, M.; Kim, S. Introduce reward-based intelligent vehicles communication using blockchain. In Proceedings of the 2017 International SoC Design Conference (ISOCC). IEEE, Seoul, South Korea, 5–8 November 2017; pp. 15–16.
39. Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet Things J. 2018, 6, 4660–4670.
40. Leiding, Benjamin, P.M.; Hogrefe., D. Self-managed and blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct, Heidelberg, Germany, 15 September 2016; pp. 137–140.
41. Reilly, E.; Maloney, M.; Siegel, M.; Falco, G. A smart city iot integrity-first communication protocol via an ethereum blockchain light client. In Proceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things (SERP4IoT 2019), Marrakech, Morocco, 3–6 April 2019; pp. 15–19.
42. Falco, G.; Siegel, J.E. Assuring Automotive Data and Software Integrity Employing Distributed Hash Tables and Blockchain. arXiv 2020 arXiv:2002.02780.
43. Rowan, S.; Clear, M.; Gerla, M.; Huggard, M.; Goldrick, C.M. Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels. arXiv 2017 arXiv:1704.02553.
44. The Mystery Behind Block Time. Available online: https:https://medium.facilelogin.com/the-mystery- behind-block-time-63351e35603a (accessed on 15 January 2020).
45. Jabbar, R., Al-Khalifa, K., Kharbeche, M., Alhajyaseen, W., Jafari, M., Jiang, S Real-time Driver Drowsiness Detection for Android Application Using Deep Neural Networks Techniques. Procedia Comput. Sci. 2018, 130, 400–407.
46. Jabbar, R., Al-Khalifa, K., Kharbeche, M., Alhajyaseen, W., Jafari, M., Jiang, S. Applied Internet of Things IoT: Car monitoring system for Modeling of Road Safety and Traffic System in the State of Qatar. In Proceedings of the Qatar Foundation Annual Research Conference 2018 (ARC'18), Doha, Qatar, 19–20 March 2018; HBKU Press: Doha, Qatar, 2018; Volume 2018.
47. Jabbar, R.; Shinoy, M.; Kharbeche, M.; Al-Khalifa, K.; Krichen, M.; Barkaoui, K. Driver Drowsiness Detection Model Using Convolutional Neural Networks Techniques for Android Application. arXiv 2020. arXiv:cs.CV/2002.03728.
48. Getting Deep Into Ethereum: How Data Is Stored In Ethereum? Available online: https://hackernoon.com/ getting-deep-into-ethereum-how-data-is-stored-in-ethereum-e3f669d96033 (accessed on 15 January 2020).
49. Wu, J.; Luo, S.; Wang, S.; Wang, H. NLES: A novel lifetime extension scheme for safety-critical cyber-physical systems using SDN and NFV. IEEE Internet Things J. 2018, 6, 2463–2475.

50. Guan, Z.; Zhang, Y.; Wu, L.; Wu, J.; Li, J.; Ma, Y.; Hu, J. APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT. J. Netw. Comput. Appl. 2019, 125, 82–92.
51. Greenspan, D.G. Ending the Bitcoin vs Blockchain Debate. MultiChain. Available online: http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/ (accessed on 15 January 2020).
52. Shomer, A. The Colored Coins Protocol. Available online: https://github.com/Colored-Coins/Colored- Coins-Protocol-Specification/wiki (accessed on 15 January 2020).
53. Maria Apostolaki, A.Z.; Vanbever, L. Hijacking bitcoin: Routing Attacks on Cryptocurrencies. Available online: https://arxiv.org/pdf/1605.07524v2.pdf (accessed on 15 January 2020).