electronics

Article

Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications

Andrei Vladyko [1], Vasiliy Elagin [2], Anastasia Spirkina [3], Ammar Muthanna [4,5] and Abdelhamied A. Ateya [4,6,*]

1 Faculty of Fundamental Training, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, 193232 Saint Petersburg, Russia; vladyko@sut.ru
2 R&D Department, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, 193232 Saint Petersburg, Russia; v.elagin@spbgut.ru
3 Infocommunication Systems Department, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, 193232 Saint Petersburg, Russia; spirkina.av@spbgut.ru
4 Department of Telecommunication Networks and Data Transmission, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, 193232 Saint Petersburg, Russia; muthanna.asa@spbgut.ru
5 Department of Applied Probability and Informatics, Peoples' Friendship University of Russia (RUDN University), 117198 Moscow, Russia
6 Department of Electronics and Communications Engineering, Zagazig University, Zagazig 44519, Sharqia, Egypt
* Correspondence: a_ashraf@zu.edu.eg; Tel.: +20-1005-237-673

Abstract: Vehicular communication is a promising technology that has been announced as a main use-case of the fifth-generation cellular system (5G). Vehicle-to-everything (V2X) is the vehicular communication paradigm that enables the communications and interactions between vehicles and other network entities, e.g., road-side units (RSUs). This promising technology faces many challenges related to reliability, availability and security of the exchanged data. To this end, this work aims to solve the scientific problem of building a vehicular network architecture for reliable delivery of correct and uncompromised data within the V2X concept to improve the safety of road users, using blockchain technology and mobile edge computing (MEC). The proposed work provides a formalized mathematical model of the system, taking into account the interconnection of objects and V2X information channels and an energy-efficient offloading algorithm to manage traffic offloading to the MEC server. The main applications of the blockchain and MEC technology in the developed system are discussed. Furthermore, the developed system, with the introduced sub-systems and algorithms, was evaluated over a reliable environment, for different simulation scenarios, and the obtained results are discussed.

Keywords: vehicular communications; vehicle-to-everything; edge computing; blockchain

Citation: Vladyko, A.; Elagin, V.; Spirkina, A.; Muthanna, A.; Ateya, A.A. Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications. *Electronics* **2022**, *11*, 173. https://doi.org/10.3390/electronics11020173

Academic Editor: Rashid Mehmood

Received: 9 December 2021
Accepted: 3 January 2022
Published: 6 January 2022

1. Introduction

The broad attention of the global community to 2030 networks, e.g., International Mobile Telecommunications-2030 (IMT-2030), has made significant contributions to the development of novel technologies and the improvement of the existing technological and technical capabilities. One of these promising networks is the intelligent transportation system (ITS) in the context of unmanned driving, automated transport and driver assistance services [1].

With the release of the fifth-generation cellular system (5G) and the current announced vision of the sixth-generation cellular system (6G), the demands for developing reliable vehicular communication systems have increased. This includes vehicle-to-everything (V2X) and vehicle-to-vehicle (V2V) technologies. V2X is the vehicular communication paradigm that enables the communications and interactions between vehicles and other network entities, e.g., road-side units (RSUs). V2X can be divided into four main types: vehicle–network

interaction (V2N), vehicle-to-vehicle interaction (V2V), vehicle–infrastructure interaction (V2I) and vehicle–human interaction (V2P) [2]. This promising technology has gained enormous interest from vehicle manufacturers, researchers and scientific communities [3]. The development of this sphere will increase the safety of road users, improve traffic flow and, consequently, reduce the negative impact on the environment.

The design and development of V2X systems face many challenges associated with the requirements, which include ultra-high availability, ultra-high reliability, ultra-low latency, high system flexibility and security. Moreover, the high mobility of such networks and the dense deployment of vehicles put high constraints on the design of these networks. Another important challenge is the lack of trust between the objects of the transport network that can negatively affect the activities and interaction, as well as leading to casualties, privacy violations and other irreversible consequences. In order to ensure the quality of services (QoS) and reduce the negative effects of the influence of unscrupulous participants in the transport interaction, blockchain is introduced to such networks at the exchange level between participants and RSUs.

Since blockchain achieves accountability and integrity between network participants, it has been introduced to secure vehicular networks communications. V2X networks have heterogeneous, massive sets of users; thus, introducing blockchain to such networks guarantees high system reliability and better information distribution. Using blockchain, the required privacy and security can be achieved for V2X networks by mitigating the link attack and detecting malicious nodes, since it can achieve a consensus without introducing a third-party [4]. Using blockchain to rate a road user is also an effective solution for V2X systems, as rating a facility allows action to be taken against offenders and encourage decent users. This ensures that misbehavior messages that create risk or reduce the efficiency of the V2X system are reduced.

The development of blockchain-based V2X systems is a prerequisite for improving the dynamic requirements of V2X services and applications, as well as expanding the range of capabilities of the services provided. It is worth noting that the provision of V2X services requires the provision of various network characteristics, such as delay, jitter, loss rate and data rates [5]. To provide and support the given service requirements, mobile edge computing (MEC) is introduced to V2X systems. MEC is cloud computing technology that moves from the centralization of massive data centers, to a distributed scheme of edge, limited, small data centers. It provides paths for data offloading, thus achieving various benefits in terms of latency, reliability, availability and flexibility.

Motivated by the described state-of-the-art technology, this work explores the problem of building a network architecture to reliably deliver correct and uncompromised data in V2X systems. This is to improve the safety of the users. A V2X framework was developed based on blockchain and MEC technologies.

The developed V2X technology provides low latency and high reliability, while taking into account the specifics of the network, the high dynamics of network topology changes and the exchange of large numbers of data. Our novel contributions can be summarized as follows:

1. Analyzing the indicators of reliability, sustainability, QoS and resource provisioning of the infrastructure facilities of the systems.
2. Designing and developing a model for the interaction of blockchain technology in the system “roadside infrastructure objects (RSU)—objects of mobile edge computing” to ensure stable and reliable delivery of information, as well as blockchain technology when organizing interaction between objects of mobile edge computing and the infrastructure of the operator’s network core.
3. Designing and developing a complex mathematical model of the system, taking into account the interconnection of objects and channels for V2X information transmission.
4. Developing an energy-efficient offloading scheme for the developed MEC-based V2X systems.
5. Performance evaluation of the developed framework for heterogeneous scenarios.

The rest of the article is structured as follows: Section 2 introduces recent related works that consider developing V2X systems based on MEC and blockchain technologies. Section 3 introduces the developed framework, including the distributed blockchain model, the MEC-based network structure and the offloading model. The performance evaluation, including the obtained results, is introduced in Section 4. Section 5 discusses the obtained results. Finally, the conclusions and future work are presented in Section 6.

2. Related Works

A large number of researchers has put the provision of data security and integrity, provision of high QoS scores and resource saving as the most important tasks of V2X technology. It is worth noting that a comprehensive approach to solving these problems for V2X systems, at the moment, according to the sources known to us, has not been presented. However, if we consider the issues in isolation, the studies below can be highlighted, which allows us to assess the importance of considering this problem.

Many researchers, for example, ref. [6], have considered the problems associated with the implementation of projects to improve transport infrastructure and have included various solutions to improve management, as well as describing the importance of using such networks.

For energy-efficient computing in the network, the limited resources of the nodes should be considered, because the high latency and low reliability of computing tasks in the network leads to repeated packet transmissions, which increases energy consumption. In a study [7], in order to reduce the latency and transmission costs of computational offload, a cloud-based MEC vehicle network offload structure was proposed to reduce the computational task execution time with high vehicle mobility. In [8], in order to reduce the execution delay and computational energy consumption, an MEC system with multiple independent tasks of joint scheduling offload optimization and transmission power allocation was proposed. A study [3] formulated the problem of economically optimal V2X service placement in a distributed cloud/frontier environment and proposed a cost- and latency-aware heuristic algorithm. The results of the study revealed a trade-off between deployment cost and latency, with latency-tolerant services generally placed in the core of the cloud to reduce costs, while latency-critical services were placed at the edge to maintain their QoS requirements. In [9], a system based on edge computing is proposed to reduce the overall latency of data transmitted between vehicles and stationary roadside devices. An algorithm was developed to manage and control the unloading of data from vehicles on border servers, taking into account the waiting time. The work simulated the system to evaluate its performance and a real experiment was conducted to test the proposed system and the developed method of unloading traffic. The study [10] plans to integrate blockchain as a robust security mechanism for 5G V2X management along with MEC. The mobile edge computing (MEC) network architecture with software-defined networking (SDN) support for V2X is described in the study [11]. To reduce the overhead of a V2X network, a problem was proposed, in which the optimal offload solution, transmission power management, sub-channel assignment and computational resource allocation scheme were given. The offloading solution was modeled as a potential game and the Nash equilibrium was confirmed by constructing a potential function.

In [12], common V2X threats are discussed and existing V2X authentication solutions are considered, while the importance of blockchain solutions in the field of critical data security for the presented networks is pointed out. In [2], an algorithm of blockchain technology operation for V2X nodes, taking into account the changes of vehicle-to-network topology due to the high mobility of vehicles, as well as an experiment that showed the numerical characteristics of resource allocation on the devices involved in the organization of V2N communication, is proposed. In [13], the authors propose a blockchain-based secure computing offloading scheme in the vehicle-to-network cloud, which included a blockchain-based trust management and a smart contract based on the DRL algorithm. In [14], the authors propose a trust model to calculate each neighbor's trust value, using the

trust value to decide whether or not to accept a data message from a neighbor. In [15–17], an analytical model for network performance evaluation is presented and the impact of blockchain technology processes on network performance is analyzed through simulations to predict traffic behavior and provide the required quality metrics, as well as the stability of network elements. These results allow further research in the organization of network interoperability and acceptable service quality to be performed and make an assessment of the relevance of technology in the field of data security and reliability.

In the study [18], the authors include an additional security mechanism based on an information-oriented evaluation of the reliability of the received danger messages. The study [19] considers different characteristics of DLT technology and concludes that system performance and security are interrelated; this trade-off is explained by the fact that various attacks are the result of increased block obsolescence rate, which, among other things, is affected by the (mis)configuration of block size and block creation interval. In [20], the authors propose a new type of local blockchain to solve critical message propagation problems in V2X/VANET. Evaluations and analyses show that the proposed local blockchain scheme can be effectively used in V2X/VANET without storage overhead.

Although the implementation of blockchain technology in V2X systems is a popular solution for security in V2X, our paper considers a fundamentally new approach compared to those studied in the literature, related to aspects of additional reliability and stability of the network; further, most studies do not consider approaches to the choice of consensus algorithms or the introduction of constraints and assumptions in the symbiosis of these technologies. In addition, the introduction of boundary computing technology is also not new to the problem of resource provisioning, but, in the current study, the application of this paradigm is more extensive and meaningful in the field of the presented symbiosis solution. The novelty of solving a number of other problems is due to the lack of a comprehensive model that allows system parameters and costs for different tasks and requirements to be varied and predicted, which is of significant importance to the implementation and use of V2X technology.

The significant number of publications of scientists from different universities and corporations on the main directions of the project confirms the magnitude and relevance of the chosen scientific problem for the infrastructure growth of developed countries. Modern studies in the world science on the main directions of the project are devoted mainly to the solution of private problems of V2X. The systematic analysis of numerous sources describing the problems of V2X suggests that the project has no scientific competitors due to the lack of comprehensive statements and interconnected solutions. Table 1 summarizes the previously introduced proposals. Most of the existing proposals utilize the paradigm of blockchain for achieving higher data security. Some of these proposals use blockchain technology with the edge computing paradigm; however, few existing proposals consider these schemes for V2X networks. The novelty of the proposed work compared to the existing proposals comes from the structure of the developed system and the developed energy-aware offloading scheme.

Table 1. Summery of related works.

Authors	V2X	Edge	Blockchain	EE	KPIs	Applications
Nellore et al. [6]	No	×	×	×	Latency, throughput	Traffic management
Zhang et al. [7]	No	√	×	×	Offloading cost	General framework
Mao et al. [8]	No	√	×	√	Energy, latency	Offloading scheme
Vladyko et al. [9]	Yes	√	×	×	Latency, reliability	General framework
Shrestha et al. [10]	Yes	√	√	×	No eval.	Review
Zhang et al. [11]	Yes	√	×	×	Offloading cost	Offloading scheme
Muhammad et al. [12]	Yes	√	×	×	No eval.	Review
Xu et al. [13]	No	√	√	×	Security	General framework
Liao et al. [14]	No	×	×	×	Security	Real-time incident
Vladyko et al. [15]	No	×	√	×	Latency	System modeling

Table 1. *Cont.*

Authors	V2X	Edge	Blockchain	EE	KPIs	Applications
Elagin et al. [16]	No	×	√	×	No eval.	Traffic modeling
Elagin et al. [17]	Yes	×	√	×	Resources utilization	System analysis
Ostermaier et al. [18]	No	×	×	×	Security	Safety applications
Kannengießer et al. [19]	No	×	√	×	No eval.	Review
Shrestha et al. [20]	Yes	×	√	×	No eval.	Real-time message exchange
Proposed work	Yes	√	√	√	Reliability, availability, latency, energy	uRLL V2X

3. V2X System Architecture When Integrating Blockchain Technology and MEC

The proposed system architecture consists of roadside participants, several RSUs, distributed MEC units and the application server. Figure 1 presents the end-to-end system structure of the developed system. The V2X system participants, e.g., vehicles, pedestrians and cyclists, are the end-devices that periodically transmit and request traffic-related information.

RSUs are used to link services to V2X objects moving on/around the road and provide route information and updates. Each RSU provides the coverage to a group of vehicles, using the appropriate communication interface. Recently, V2X communications implemented using two main technologies, namely, 3GPP-based technology and dedicated short range communications (DSRC). IEEE 802.11p is the common DSRC that is widely used for V2X applications, while cellular vehicle-to-everything (C-V2X) is the alternative technology introduced by the 3GPP [21].

Distributed MEC units are introduced at the edge of the access network, by connecting each RSU with an MEC unit. These edge units provide computing resources to roadside participants. Moreover, they implement the developed offloading scheme to manage the network traffic in an energy-efficient way.

3.1. V2X

In recent decades, the dedicated vehicle network has become a major network technology for the comfort and safety of drivers in vehicle environments. However, new applications and services require major changes in the underlying network models and calculations, which requires new road network planning [22].

Thus, the emergence of critical messages and applications related to the safety of road users, which leads to high performance requirements and strict reliability of data transmission, should be noted. The transmitted messages can be divided into two categories, safety messages and general-purpose (non-safety-related) messages. For information about any emergency, vehicles can transmit or broadcast messages with high priority and high requirements. For information that is not an emergency, the requirements can be lowered. Based on the different requirements, V2X services can be divided into several basic types [23,24].

Depending on the severity of the emergency, event messages are divided into different levels according to priority, where level 1 defines critical event messages with the highest priority, etc.

The primary goal of the vehicle network is to accurately disseminate information in a short time, with the required reliability and safety. There is a high risk that modern vehicles are subjected to cyber-attacks targeting vehicular communications [25]. Due to inaccurate information sent by malicious vehicles, some important messages cannot be accurately disseminated in real time, resulting in damage to other traffic participants. Another problem could be the theft of important and sensitive information from traffic participants.

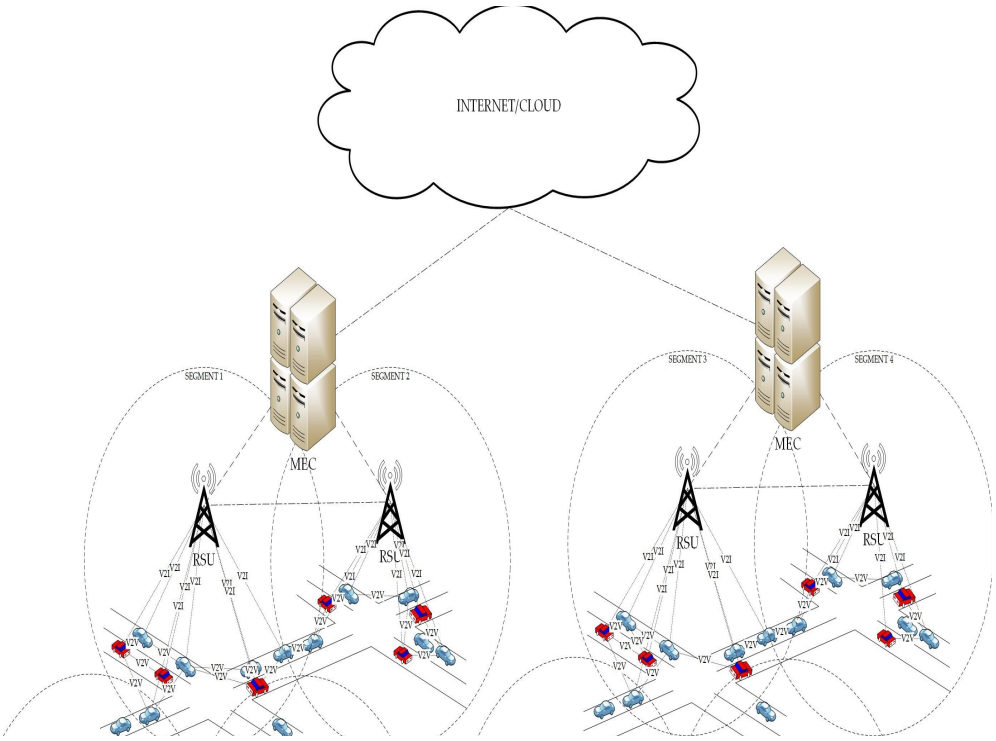

Figure 1. The architecture of the proposed system.

3.2. Application of Blockchain Technology between Road Users and RSUs

In the case of V2X, promising blockchain technology can be used to manage information trustworthiness, as event information would be stored in a publicly accessible blockchain. This technology can be applied in a variety of circumstances, such as the reliable transfer of information between network objects, the assessment of a road user's rating and credibility with high node mobility.

Blockchain can solve major problems faced by V2X systems and provide security for the distribution of critical information. Using blockchain to reliably transmit information is important when transmitting and avoiding loss or distortion that could lead to negative consequences. Blockchain technology relies on rules and concepts to avoid these consequences. Due to the design of blockchain trust management, it can be successfully applied between nodes with decentralized systems.

Malicious nodes can infiltrate the network and spread false information on the network, causing the transport network to fail. Using blockchain to rate a road user is also an effective solution for use in the V2X system, as rating a facility would allow action to be taken against offenders and encourage decent users. This would ensure that misbehavior messages that create risk or reduce the efficiency of the V2X system are reduced.

The use of algorithms on trust management and separation of priorities allows traffic participants to determine, with high probability, whether the received message is reliable. Thus, for objects with a high reputation rating, the information would be accepted faster, since the quality of the data depends on the reputation of the object. The trust value of the network participants is determined based on the scores obtained from past behavior, which are attached and stored in the system using blockchain technology. Thus, two parameters would be used in messaging—first, the event information itself and, second, the priority of the message based on the service category and on the reputation of the object (rep). This method would allow a more objective perception of the real situation to be obtained, encourage users to behave decently and consistently record events for further processing and use.

To organize this process, the authors propose to use blockchain with the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm, which is responsible for efficient

operation in asynchronous networks, allowing consensus to be reached even if some nodes in the network do not respond or give wrong information. This algorithm involves selecting two types of nodes—leader and backup nodes. Each node in the network maintains its own internal state and, when it receives a message, it performs calculations and prepares a decision on the newly received message. The individual decision of each node is sent to the node leader, who confirms the credibility of the new message based on the decisions of all nodes. The leader in our system is proposed to use the RSU, while the redundant nodes are traffic participants connected to the V2X system.

The procedures for calculating, verifying and storing a blockchain-based trust score are shown below.

3.2.1. Registration and Initialization

Each road user with an electronic device must register with the authority, which is the trusted official unit that manages the security parameters and keys of all organizations, and obtain a public key, a private key and identity certificates. Each participant is also assigned a reputation based on offenses and experience (for drivers of vehicles); the rating is generated from 0.1 to 1.0, where 1.0 is the highest rating indicator value.

3.2.2. Receiving and Synchronization of Primary Data

After the necessary parameters are assigned and the user is verified, the data are synchronized between the certification centers and the user, with some data automatically synchronized to the blockchain (rating, device ID, etc.) and to the device.

3.2.3. Initializing a Network Member

When a device enters the range of the next RSU, the device automatically transmits its data (device ID). The participants, in turn, check the information and receive rating data; if the device is not found in the registry, the information is transmitted to the RSU for further decision, with the device being considered an intruder until the reasons are clarified. However, if the device is marked and initialized correctly, it is considered a full member of the network.

3.2.4. Messaging

When transmitting information, the device forms a message in the form of a transaction, while writing the reputation rating value and the priority of the situation into it. Transactions are written to a block and transmitted to all participants in the network. The higher the reputation and priority of the message are, the faster the decision to accept it. A block is fixed when more than 2/3 of validators pre-fix the same block in the same round for transactions with coefficient (k) below 0.6 and 2/4 for transactions with coefficient (k) above or equal to 0.6.

$$k = (\frac{1}{prio}) * rep \quad (1)$$

If the message is compromised or incorrect, the message sender's behavior is then transmitted to the blockchain and reported to the trusted authority. Thus, the reputation of the sender of the message is degraded.

Most modern blockchain systems are a single-chain architecture. Thus, each node has to perform multiple duplicate computational tasks, resulting in a loss of energy. In addition, its performance degradation becomes more evident when traffic peaks occur [26].

In the case of V2X, there is no need to share blocks beyond the region. To solve the scalability problem, the proposed architecture uses a segmentation approach. Segmentation is the division of the workload of a blockchain network over a peer-to-peer network, so that each node is not responsible for the transaction load of the entire network [27]. This allows different segments to process transactions in parallel to increase throughput, which speeds up validation processes as well as block validation in time-dependent situations while maintaining interoperability. According to the high mobility of independent subnet

nodes, different subnets can have different numbers of nodes and block generation times. The Chameleon, OmniLedger [28], or Elastico [29] solution is proposed as the basis for object interconnection in segmentation.

The architecture of the main chain (multi-chain) is shown in Figure 2. The architecture is based on a main chain, which manages multiple semi-independent segments.

When a subchain is created, the relevant information is reflected from the main chain to the corresponding subchains in such a way that the subchains correspond to the states of the main chain. The algorithm for generating data chains is presented in Algorithm 1. In the chains of segments, the data of one block are stored in a complete chain of a certain period of time, for example, one day or one week, and the previous blocks are stored in multi-chains. It is worth noting that a segmented system model must account for the negligible probability that any segment is compromised.

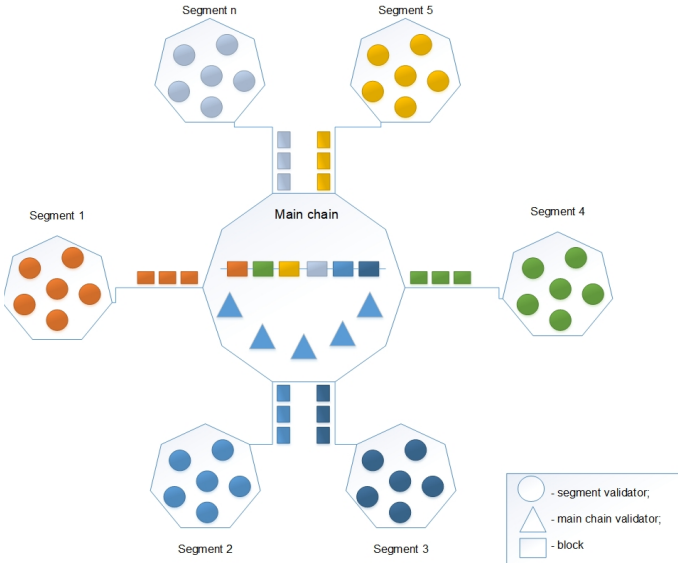

Figure 2. Multi-chain architecture.

Algorithm 1 EETO Algorithm

1: **Initialization**: Each vehicle i is connected to a single RSU j and the offloading decision is initialized with local execution $\alpha_{i,0} = 1$.
2: **for all** RSUs j and at time slot t **do**
3: Send the available resources to the core network.
4: **for all** vehicle i **do**
5: Send the requirements for each task $\{a_i, c_i, p_i\}$ and the computational capability f_i^l to the core network.
6: **end for**
7: **end for**
8: Obtain the optimal offloading value α^* through solving Equation (13).
9: Send the offloading decision values to each vehicle i.

Additionally, the authors do not deny that, in the future, a Cosmos network-type protocol could be used instead of segmentation [30], but, at the time of writing, these types of solutions are only in the development stage and have no final solution.

If we consider the procedure of selecting the entry and exit of the segment, the need to dynamically update the information based on such parameters as the number of devices in the segment and the distance from the RSU should be noted.

3.3. Integration of Mobile Edge Computing (MEC) into the V2X System

Limited resources, a dynamic road user environment and long distances between cloud servers make it difficult to support computationally intensive services and cause problems such as additional latency, jitter and high power consumption [31]. To solve these problems, the European Telecommunications Standards Institute, in 2014, proposed the use of mobile peripheral computing [3]. Cloud-based models require the transmission and storage of V2X system object data in specialized data centers, which increases the likelihood of information leakage or loss and long latency, which can lead to accidents [24]. In addition to this, the devices require additional services, such as computing and updating the user rating and network segment selection, which is a very time-consuming process; further, it becomes necessary to resort to mobile edge computing technology. Since we are dealing with emergency event messages, the timeliness of the dissemination of messages is of paramount importance.

It should be noted that, when the RSU load is high, MEC can perform load balancing to other RSUs or to its own facilities. We consider each unloading task as a service to the edge infrastructure. Moreover, as the number of network participants and events increases, the energy consumed for computation and data transmission increases.

The loading pattern of RSUs and MEC depends on the corresponding traffic flow in that region. It is assumed that multiple RSUs share common edge server resources. To select segments and reduce service delays for excessive loads, it is necessary to expand the computational capacity of MEC. It is important to provide a balanced unloading scheme for different RSUs and to provide decision-making capacity for messages that require high reliability and system responsiveness.

It is necessary to consider that attackers could intervene to manipulate the results of the computation, which could have serious consequences in the operation of the requested algorithm, resulting in the need to allocate additional resources for a particular service request. In the proposed model, MEC using blockchain technology based on smart contracts between service providers and mobile peripheral computing devices stores data related to each service request, such as the amount of resources allocated, hash of computation results and associated object identifiers and timestamps. This chain provides transparency in resource allocation and automates each process through smart contract mechanisms to reduce human intervention. MEC servers provide services and send the results of calculations to the appropriate RSUs and the cloud.

3.4. System Model

In this work, we consider a multi-level blockchain-enabled MEC system for V2X networks, in which our environment consists of three main planes, shown in Figure 1. In the first plane, we assume $\mathbb{A} = \{1, 2, \ldots, M\}$ as a set vehicles that are moving across a single-way road and each vehicle has a computation task that needs to be accomplished, whereas, in the second plane, a set of $\mathbb{B} = \{1, 2, \ldots, N\}$ roadside units (RSUs) are distributed across the road and connected with edge computing servers (RSUs and edge servers are interchangeably used in this paper), which can provide the computation and storage capabilities for vehicles. Moreover, in this plane, we configured the blockchain architecture over the edge servers to address the privacy and security issues for the set of vehicles during the data offloading process. Last, in the third plane, we have a centralized cloud data center connected with the edge servers through the core IP network, which is responsible for managing the edge servers.

In this study, we consider $\mathbb{S} = \{0, 1, 2, \ldots, N, N+1\}$ as the computing server set that is utilized to process the vehicles' task, in which 0 denotes that the task is to be processed locally at the vehicle itself and $N+1$ denotes that the task is to be processed at the cloud server. In addition, $\alpha_{i,j} \in \{0, 1\}$ is used to denote the decision of offloading of vehicles' task, in which ($\alpha_{i,0} = 1$) and ($\alpha_{i,N+1} = 1$) mean that the task is to be processed locally and remotely at the cloud server, respectively, whereas ($\alpha_{i,j} = 1, \forall_j \in [1..N]$) means that the vehicles' task is to be processed remotely at one of the RSUs. Moreover, the computation

task for the vehicle i can only be processed at one of the servers (including server 0), while $\sum_{j=0}^{N+1} \alpha_{i,j} = 1$. Guided by the intuition in [32,33], in this paper, the movement and trajectories of the vehicles along the road can be predicted.

The following subsections present more details about the communication and computation models and the formulation of a multi-level blockchain-enabled MEC system for the V2X network problem.

3.4.1. Communication Model

This subsection starts with an introduction to the model of communication, where the system environment is composed of $\mathbb{B}$ and $\mathbb{A}$ sets of RSUs and vehicles, respectively. In addition, each vehicle has a computation task to be accomplished, which can be identified using a tuple $\{a_i, c_i\}$. More specifically, a_i is used to denote the size of transferred data (i.e., code and parameters) for the computation task and c_i is used to denote the CPU cycle number demanded to complete the computation task. Guided by the works [34,35], the a_i and c_i' values can be obtained through task execution profiling.

Regarding the intuition shown in [36], in this study, we chose to disregard the consumption overhead in terms of time and energy for transmitting the result back to the vehicles, since the output data are few, relative to the input data.

Note that, in the case of multiple vehicle transmissions in the same cell, the orthogonal frequency-division multiplexing method was utilized to mitigate the intracellular interference [36,37]. In addition, according to Shannon's law [38], the uplink data rate for communication between the vehicle i and the connected RSU j is given by

$$r_{i,j} = B_{i,j} log_2(1 + \frac{p_i g_0^2}{\omega B_{i,j}}) \tag{2}$$

where $B_{i,j}$ indicates the uplink channel bandwidth, p_i indicates the vehicle i's transmission power and ω and g_0 indicate the noise power density and the corresponding channel gain between the vehicle and the connected RSU.

3.4.2. Computation Model

In this subsection, the computation model is presented, where our system environment is composed of a set of vehicles $\mathbb{A}$ that is connected t a set of RSUs $\mathbb{B}$ via a wireless channel. Additionally, each vehicle i has an intensive task to be processed locally at the vehicle or preserved as a set of transactions and then offloaded to one of the available servers (i.e., edge or cloud) through the blockchain architecture. Consequently, the computation overhead in terms of time and energy for processing the vehicles' tasks, wherever locally or remotely, is discussed in the next subsections.

Local Execution Approach

The local execution approach takes into account that different vehicles may have different capabilities of computation. Moreover, each vehicle is to execute its task locally.

Therefore, for each vehicle i, the execution time and energy consumption for performing the computation tasks locally can be calculated accordingly, as follows:

$$T_i^l = \frac{c_i}{f_i^l} \tag{3}$$

$$E_i^l = \vartheta_i c_i \tag{4}$$

where the computational capability of vehicle i in CPU cycles per second is indicated by f_i^l and the energy consumed per CPU cycle is represented by ϑ_i.

Remote Execution Approach

As part of the remote execution approach, the computation task for vehicle i is offloaded and executed on one of the connected servers j.

Therefore, for each vehicle i, the execution time for performing the computation tasks remotely at the edge or cloud servers can be computed accordingly, as follows:

$$T_i^e = T_i^{tr} + T_i^{e\_ex} \tag{5}$$

$$T_i^c = T_i^{tr} + \Delta + T_i^{c\_ex} \tag{6}$$

where the propagation delay for edge and cloud communication is indicated by Δ. Moreover, the transmission, edge and cloud execution are indicated by T_i^{tr},$T_i^{e\_ex}$ and $T_i^{c\_ex}$, respectively, which are expressed as

$$T_i^{tr} = \frac{a_i}{r_{i,j}} \tag{7}$$

$$T_i^{e\_ex} = \frac{c_i}{f_i^e} \tag{8}$$

$$T_i^{c\_ex} = \frac{c_i}{f_i^c} \tag{9}$$

where the computational capability allocated for each vehicle i at the RSUs and cloud are indicated by f_i^e and f_i^c, respectively.

Subsequently, for each vehicle i, the energy consumption for transmitting the computation tasks remotely at the edge or cloud servers can be computed accordingly, as follows:

$$E_i^{tr} = p_i T_i^{tr} \tag{10}$$

In this study, the computational resources of each edge server are equal and assumed to be equally shared between all the connected vehicles.

Finally, based on Equations (3), (4) and (8)–(10), the total time and energy for performing all the computation tasks of vehicle i can be respectively computed as

$$T_i = \alpha_{i,0} T_i^l + \alpha_{i,N+1} T_i^c + \sum_{j=1}^{N} \alpha_{i,j} T_i^e \tag{11}$$

$$E_i = \alpha_{i,0} E_i^l + \sum_{j=1}^{N+1} \alpha_{i,j} E_i^{tr} \tag{12}$$

3.5. Problem Formulation

This section investigates the problem formulation of our system, in which reducing the total energy overhead for a multi-level blockchain-enabled MEC system for V2X networks is the main goal. Therefore, based on the above models (i.e., communication and computation), the models can be formulated as a constrained optimization, as follows:

$$\begin{aligned} \min_{\alpha} \quad & \sum_{i=1}^{M} E_i \\ & E_i - E_i^l \leq 0, \qquad C1 \\ & T_i - T_i^l \leq 0, \qquad C2 \\ & \sum_{j=0}^{N+1} \alpha_{i,j} = 1, \qquad C3 \\ & \alpha_{i,j} \in \{0,1\} \qquad C4 \end{aligned} \tag{13}$$

This optimization problem aims to reduce the energy consumption of the entire system through task offloading. In addition, the upper limit for energy consumption and time are addressed through the first two constraints (i.e., C1 and C2, respectively), whereas the execution limit (i.e., only one time) for each vehicle's i task is guaranteed via constraint C3. Finally, the binarization of the offloading decision variable is guaranteed through constraint C4.

In the case of linear objective functions and constraints, the problem solution is determined through finding the best value for the decision offloading variable α^*. Therefore, the branch and bound technique was used in this study, in accordance with [39,40], to solve this problem.

Problem Solution Using Energy-Efficient Task Offloading (EETO) Algorithm

This subsection describes our energy-efficient task offloading (EETO) algorithm to determine the optimal offloading decision of a multi-level blockchain-enabled MEC system for V2X networks. First, each RSU sends an information summary of their vehicles, including vehicles' number, available computation resources and transmission rate, to the core network. In addition, each vehicle also send the tasks' requirements, including tasks' CPU cycles, input size and transmission power, to the core network. Next, based on Equation (13), the core network can derive the optimal offloading decision for each vehicle's task through the problem solution. Finally, each RSU sends the offloading decision for each vehicle which determines wherever the task is to be executed (i.e., locally, edge or cloud server). The detailed process for energy-efficient task offloading is outlined in Algorithm 1.

4. Performance Evaluation

In this part, we present the developed blockchain-MEC V2X system evaluated for various scenarios. The evaluation process was carried out over the NS-3 environment, with the highway mobility model. Simulation Urban Mobility (SUMO) is an open-source environment used to provide the required vehicle mobility, with synchronization and control of NS-3. TraCI API was used to build the module that achieves such integration. The trajectory files out of the SUMO were fed to NS-3 to define the nodes' mobility. The FastChian NS-3-based tool was used to implement the developed blockchain scheme, with the steps introduced in [41].

Table 2 provides the considered simulation parameters. There were seven MEC servers considered for the simulation process, with the specifications introduced in Table 2. The communication was assumed to be carried over the C-V2X Mode 4 interface. Vehicles were located randomly, with the specifications introduced in Table 2, over a four-lane bi-directional road of 5 km in length. Each vehicle was assigned a workload equivalent to the workload of real tasks. The considered workloads were UDP-based. The number of deployed vehicles, N, was assigned three values, as the system was simulated for 200, 400 and 600 vehicles to check the effect of the traffic increase on the performance of the developed blockchain–MEC V2X system. Moreover, three densities of vehicles were considered for the simulation process to evaluate the effect of the change in vehicle density, TD, on the overall system performance.

The first performance metric considered in the evaluation process of the developed blockchain–MEC V2X was the communication overhead. Two systems were considered for such performance evaluation, system (I) and system (II). The first system, i.e., system (I), was a blockchain–MEC V2X system with no clustering priorities, as each vehicle was responsible for its communication. Thus, in this system, vehicles communicated individually. In system (II), there was a clustering priority, as nodes with common behavior, e.g., speed and direction, selected a cluster head to take the responsibility of the communication. Thus, in system (II), a limited number of vehicles, i.e., cluster heads (leader nodes), was responsible for communication. For system (I), the communication overhead was at a higher level than for system (II).

Figure 3 presents the percentage of the communication overhead for system (II) compared to system (I), for three different cases of traffic density. As the traffic density increased, the communication overhead increased by an average of 13% for each 10% of traffic density increase. Furthermore, clustering reduced the communication overhead of the developed blockchain–MEC V2X system; however, when the percentage of cluster heads (leader nodes) reached 70% of all vehicles in the cluster, the clustering was efficient no more and the com-

munication overhead was the same as with no clustering. Figure 4 presents the percentage of the communication overhead with the number of cluster heads, for three different values of the average number of vehicles in the network. As the number of vehicles increased in the network, the average communication overhead increased. Moreover, to evaluate the effect of vehicle mobility on the developed blockchain–MEC V2X, the communication overhead was measured for different values of vehicle mobility. Figure 5 presents the communication overhead of system (II), compared to system (I), with the change in vehicle mobility; at cluster-head percentages of 10, 20 and 30 from the total number of cluster members, the communication overhead increased linearly till a mobility of 60 km/h, then the increase in vehicle mobility produced a higher increase in the communication overhead.

Table 2. Simulation parameters.

Parameter	Value
No. of vehicles (N)	200, 400, 600
Number of MEC units	7
Number of lanes	4
Road length	5 km
Density of vehicles (TD)	0.1, 0.2, 0.3 veh/m
MEC placement	*equidistant*
Packet transmission frequency	10 Hz
Simulation time	150 s
Streaming service bandwidth	$\in$[10, 2048] (KB/S)
Channel bandwidth	10 MHz
Packet size	190 bytes
Vehicle task energy	$\in$[20, 80] (watt/s)
Transmit power	23 dBm
Maximum work load (MEC)	50 events/s
Storage/RAM	2048 MB
Storage/HDD	5 GB
Processing/CPU	$\in$[0.7, 2.5] GHz

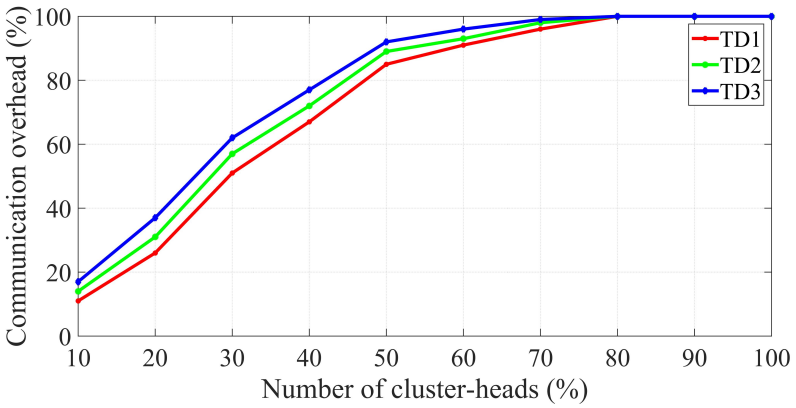

Figure 3. Percentage of the communication overhead with the change in the number of cluster heads, for different values of traffic density.

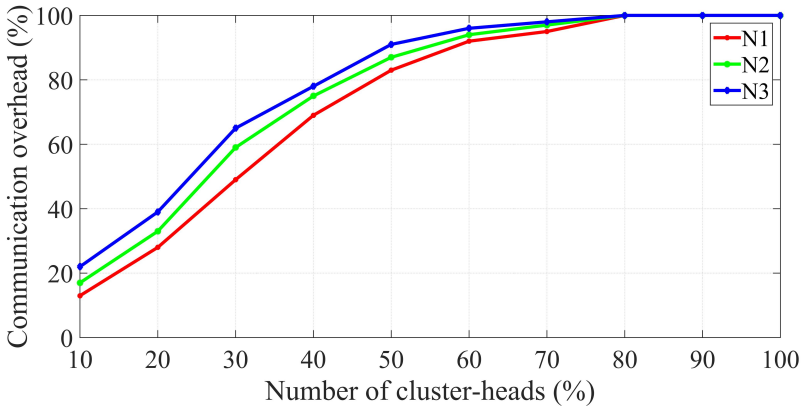

Figure 4. Percentage of the communication overhead with the change in the number of cluster heads, for different values of number of deployed vehicles.

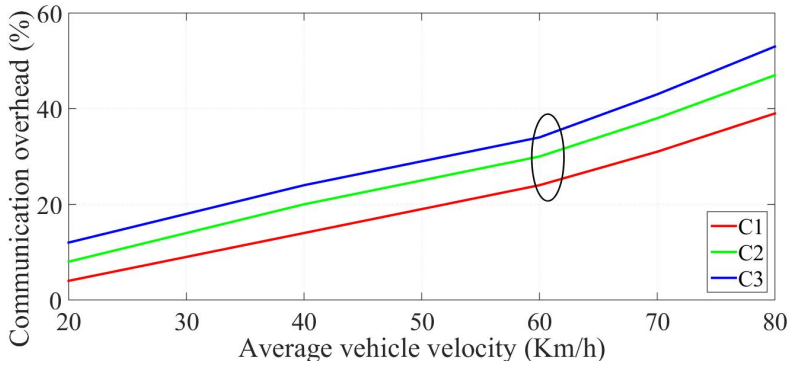

Figure 5. Percentage of the communication overhead with the change in the vehicle velocity.

The percentage of blocked tasks compared to the total number of computing tasks was detected for the developed blockchain–MEC V2X system with the developed offloading scheme and for the optimized offloading scheme. Figure 6 provides the average percentage of blocked tasks for the three considered cases, for different values of number of vehicles. Each case represents a system; case (1) represents the system with local execution and no offloading scheme. The second case, case (2), represents the developed system with the developed offloading scheme, while the third case, case (3), was introduced for the developed system with the optimized offloading scheme. The optimized offloading scheme achieved the highest performance of task handling, even with the increase in the number of vehicles. Figure 7 provides the average percentage improvement of latency performance of the developed blockchain–MEC V2X compared with the traditional system, for three values of deployed vehicles. Moreover, the latency performance improvement of the optimized blockchain–MEC V2X is introduced in Figure 7. The optimized blockchain–MEC V2X achieved an average improvement of the latency performance of 39% compared with the traditional systems. The developed offloading scheme with blockchain–MEC V2X improved the energy efficiency of the system by reducing the energy consumption of task handling. Figure 8 provides the average percentage improvement of the energy performance for both systems, the blockchain–MEC V2X and the optimized blockchain-MEC V2X, compared with the traditional systems, for three values of deployed number of vehicles. The optimized blockchain–MEC V2X achieved an average improvement of energy efficiency of 36% compared to the traditional V2X systems.

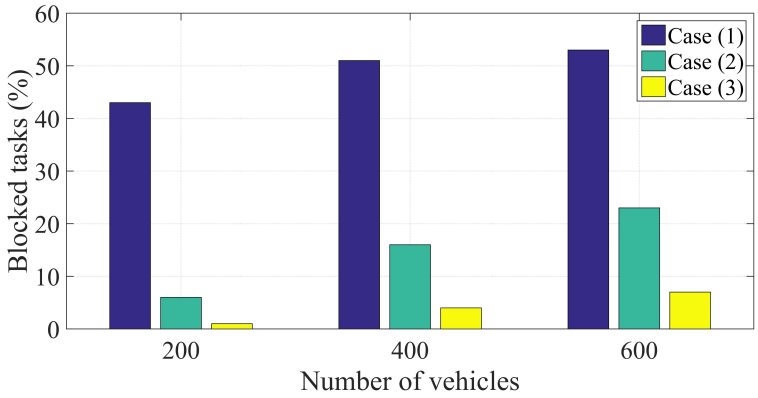

Figure 6. Average percentage of blocked tasks for different values of deployed vehicles.

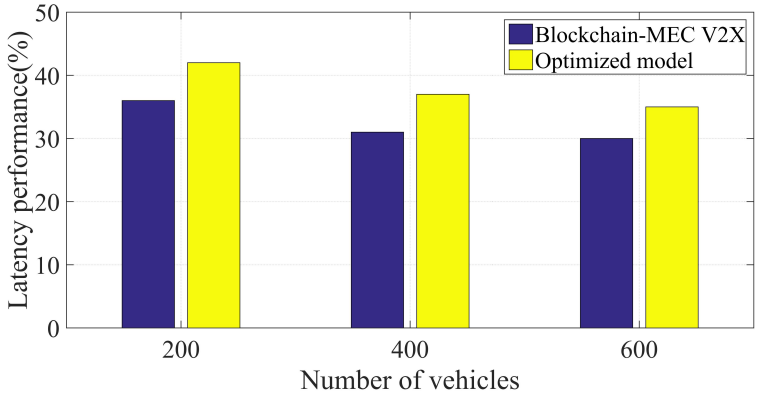

Figure 7. Latency performance of the developed systems compared with the traditional systems, for different values of deployed vehicles.

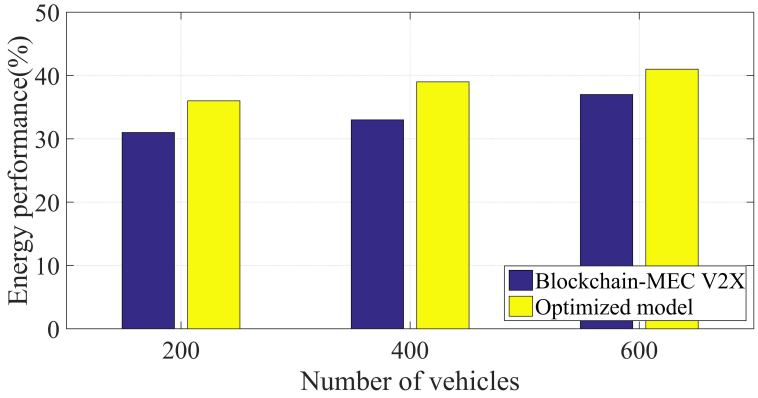

Figure 8. Energy performance of the developed systems compared with the traditional systems, for different values of deployed vehicles.

5. Discussion

The developed blockchain–MEC V2X system achieved higher reliability than existing V2X models. The optimized blockchain–MEC V2X reduced the percentage of blocked tasks by an average of 41% compared to traditional V2X systems. This is due to introducing resources at the edge in an optimized way. Another performance improvement achieved by the developed blockchain–MEC V2X system is latency efficiency. The optimized model of the developed system achieved an improvement of average latency efficiency of 39% compared to traditional systems. The introduction of MEC servers reduced communication latency and, with the optimized offloading scheme, the resources were utilized in a higher-efficient way that achieved this latency performance improvement. Furthermore, the optimized model of the developed V2X system achieved higher energy efficiency than

traditional systems, by an average of 36%. This is due to task offloading, which was performed in an optimized way that achieved the minimum energy consumption in handling each task. The developed system is limited to MEC resources; however, increasing such resources affects the overall cost of the network, including both OPEX and CAPEX.

6. Conclusions

The article provides a framework of V2X based on distributed edge computing (MEC) and blockchain technologies. A model for the interaction of blockchain technology in the system was introduced in a way that achieved the required level of security. In the developed framework, each RSU is connected to an edge computing server, which is integrated with the introduced blockchain model. A computational offloading scheme was developed and introduced in a way that reduced the latency in handling computing tasks. The model was optimized in terms of energy to reduce the overall energy consumption. The developed blockchain–MEC model was evaluated over an NS-3 environment for various simulation scenarios and the results validate the system in terms of reliability, latency and energy efficiency. The optimized model of the developed system achieved higher latency efficiency by 39% and higher energy efficiency by 36% than traditional V2X systems.

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

Funding: Research funded by Ministry of Digital Development, Communications and Mass Media of the Russian Federation, contract number ГЗ3-1-26/9 (Moscow, Russia).

Acknowledgments: The researcher A.A. Ateya was funded by the Ministry of Higher Education of the Arab Republic of Egypt.

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

References

1. Lin, S.C.; Chen, K.C.; Karimoddini, A. SD-VEC: Software-Defined Vehicular Edge Computing with Ultra-Low Latency. *arXiv* **2021**, arXiv:2103.14225.
2. Muthanna, A.; Shamilova, R.; Ateya, A.A.; Paramonov, A.; Hammoudeh, M. A mobile edge computing/software-defined networking-enabled architecture for vehicular networks. *Internet Technol. Lett.* **2020**, *3*, e109. [CrossRef]
3. Moubayed, A.; Shami, A.; Heidari, P.; Larabi, A.; Brunner, R. Cost-optimal v2x service placement in distributed cloud/edge environment. In Proceedings of the 2020 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)(50308), Thessaloniki, Greece, 12–14 October 2020; pp. 1–6.
4. Rawat, D.B.; Doku, R.; Adebayo, A.; Bajracharya, C.; Kamhoua, C. Blockchain enabled named data networking for secure vehicle-to-everything communications. *IEEE Netw.* **2020**, *34*, 185–189. [CrossRef]
5. Mei, J.; Wang, X.; Zheng, K. Intelligent network slicing for V2X services toward 5G. *IEEE Netw.* **2019**, *33*, 196–204. [CrossRef]
6. Nellore, K.; Hancke, G.P. Traffic management for emergency vehicle priority based on visual sensing. *Sensors* **2016**, *16*, 1892. [CrossRef] [PubMed]
7. Zhang, K.; Mao, Y.; Leng, S.; He, Y.; Zhang, Y. Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading. *IEEE Veh. Technol. Mag.* **2017**, *12*, 36–44. [CrossRef]
8. Mao, Y.; Zhang, J.; Letaief, K.B. Joint task offloading scheduling and transmit power allocation for mobile-edge computing systems. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017; pp. 1–6.
9. Vladyko, A.; Khakimov, A.; Muthanna, A.; Ateya, A.A.; Koucheryavy, A. Distributed edge computing to assist ultra-low-latency VANET applications. *Future Internet* **2019**, *11*, 128. [CrossRef]
10. Shrestha, R.; Nam, S.Y.; Bajracharya, R.; Kim, S. Evolution of V2X Communication and Integration of Blockchain for Security Enhancements. *Electronics* **2020**, *9*, 1338. [CrossRef]
11. Zhang, H.; Wang, Z.; Liu, K. V2X offloading and resource allocation in SDN-assisted MEC-based vehicular networks. *China Commun.* **2020**, *17*, 266–283. [CrossRef]

12. Muhammad, M.; Safdar, G.A. Survey on existing authentication issues for cellular-assisted V2X communication. *Veh. Commun.* **2018**, *12*, 50–65. [CrossRef]
13. Xu, S.; Guo, C.; Hu, R.Q.; Qian, Y. BlockChain Inspired Secure Computation Offloading in a Vehicular Cloud Network. *IEEE Internet Things J.* **2021**, doi:10.1109/JIOT.2021.3054866. [CrossRef]
14. Liao, C.; Chang, J.; Lee, I.; Venkatasubramanian, K.K. A trust model for vehicular network-based incident reports. In Proceedings of the 2013 IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC), Dresden, Germany, 2–3 June 2013; pp. 1–5.
15. Vladyko, A.; Spirkina, A.; Elagin, V. Towards Practical Applications in Modeling Blockchain System. *Future Internet* **2021**, *13*, 125. [CrossRef]
16. Elagin, V.; Spirkina, A.; Levakov, A.; Belozertsev, I. Blockchain behavioral traffic model as a tool to influence service IT security. *Future Internet* **2020**, *12*, 68. [CrossRef]
17. Elagin, V.; Spirkina, A.; Buinevich, M.; Vladyko, A. Technological aspects of blockchain application for vehicle-to-network. *Information* **2020**, *11*, 465. [CrossRef]
18. Ostermaier, B.; Dotzer, F.; Strassberger, M. Enhancing the security of local dangerwarnings in vanets-a simulative analysis of voting schemes. In Proceedings of the Second International Conference on Availability, Reliability and Security (ARES'07), Vienna, Austria, 10–13 April 2007; pp. 422–431.
19. Kannengießer, N.; Lins, S.; Dehling, T.; Sunyaev, A. Mind the gap: Trade-offs between Distributed Ledger Technology characteristics. *arXiv* **2019**, arXiv:1906.00861.
20. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. *Digit. Commun. Netw.* **2020**, *6*, 177–186. [CrossRef]
21. Haider, A.; Hwang, S.H. Adaptive Transmit Power Control Algorithm for Sensing-Based Semi-Persistent Scheduling in C-V2X Mode 4 Communication. *Electronics* **2019**, *8*, 846. [CrossRef]
22. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A distributed blockchain based vehicular network architecture in smart city. *J. Inf. Process. Syst.* **2017**, *13*, 184–195.
23. Campolo, C.; Molinaro, A.; Iera, A.; Menichella, F. 5G network slicing for vehicle-to-everything services. *IEEE Wirel. Commun.* **2017**, *24*, 38–45. [CrossRef]
24. Islam, S.; Badsha, S.; Sengupta, S.; La, H.; Khalil, I.; Atiquzzaman, M. Blockchain-Enabled Intelligent Vehicular Edge Computing. *IEEE Netw.* **2021**, *35*, 125–131. [CrossRef]
25. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communications. *Veh. Commun.* **2020**, *23*, 100214. [CrossRef]
26. Yu, Y.; Liang, R.; Xu, J. A scalable and extensible blockchain architecture. In Proceedings of the 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 17–20 November 2018; pp. 161–163.
27. Aiyar, K.; Halgamuge, M.N.; Mohammad, A. Probability distribution model to analyze the trade-off between scalability and security of sharding-based blockchain networks. In Proceedings of the 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2021; pp. 1–6.
28. He, G.; Su, W.; Gao, S. Chameleon: A scalable and adaptive permissioned blockchain architecture. In Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, China, 15–17 August 2018; pp. 87–93.
29. Luu, L.; Narayanan, V.; Zheng, C.; Baweja, K.; Gilbert, S.; Saxena, P. A secure sharding protocol for open blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 17–30.
30. Cosmos. Interchain Standards. Available online: https://github.com/cosmos/ibc (accessed on 17 October 2021).
31. Li, D.; Xu, S.; Li, P. Deep reinforcement learning-empowered resource allocation for mobile edge computing in cellular v2x networks. *Sensors* **2021**, *21*, 372. [CrossRef] [PubMed]
32. Zhao, Z.; Guardalben, L.; Karimzadeh, M.; Silva, J.; Braun, T.; Sargento, S. Mobility prediction-assisted over-the-top edge prefetching for hierarchical VANETs. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 1786–1801. [CrossRef]
33. Yao, L.; Chen, A.; Deng, J.; Wang, J.; Wu, G. A cooperative caching scheme based on mobility prediction in vehicular content centric networks. *IEEE Trans. Veh. Technol.* **2017**, *67*, 5435–5444. [CrossRef]
34. Lyu, X.; Tian, H. Adaptive receding horizon offloading strategy under dynamic environment. *IEEE Commun. Lett.* **2016**, *20*, 878–881. [CrossRef]
35. Liu, F.; Huang, Z.; Wang, L. Energy-efficient collaborative task computation offloading in cloud-assisted edge computing for IoT sensors. *Sensors* **2019**, *19*, 1105. [CrossRef]
36. Elgendy, I.A.; Zhang, W.; Tian, Y.C.; Li, K. Resource allocation and computation offloading with data security for mobile edge computing. *Future Gener. Comput. Syst.* **2019**, *100*, 531–541. [CrossRef]
37. Deb, S.; Monogioudis, P. Learning-based uplink interference management in 4G LTE cellular systems. *IEEE/ACM Trans. Netw. (TON)* **2015**, *23*, 398–411. [CrossRef]
38. Chatzinotas, S.; Imran, M.A.; Hoshyar, R. On the multicell processing capacity of the cellular MIMO uplink channel in correlated Rayleigh fading environment. *IEEE Trans. Wirel. Commun.* **2009**, *8*, 3704–3715. [CrossRef]
39. Hao, Y.; Chen, M.; Hu, L.; Hossain, M.S.; Ghoneim, A. Energy efficient task caching and offloading for mobile edge computing. *IEEE Access* **2018**, *6*, 11365–11373. [CrossRef]

40. Zhang, W.Z.; Elgendy, I.A.; Hammad, M.; Iliyasu, A.M.; Du, X.; Guizani, M.; Abd El-Latif, A.A. Secure and Optimized Load Balancing for Multitier IoT and Edge-Cloud Computing Systems. *IEEE Internet Things J.* **2020**, *8*, 8119–8132. [CrossRef]
41. Khakurel, U.; Rawat, D.; Njilla, L. FastChain: Lightweight Blockchain with Sharding for Internet of Battlefield-Things in NS-3. In Proceedings of the 2019 IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA, 11–12 November 2019; pp. 241–247.