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; elagin.vas@gmail.com
[3] Infocommunication Systems Department, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, 193232 Saint Petersburg, Russia; spirkina.av@gmail.com
[4] Department of Telecommunication Networks and Data Transmission, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, 193232 Saint Petersburg, Russia
[5] Department of Applied Probability and Informatics, Peoples' Friendship University of Russia (RUDN University), 117198 Moscow, Russia; ammarexpress@gmail.com
[6] Department of Electronics and Communications Engineering, Zagazig University, Zagazig, Sharqia 44519, Egypt; a_ashraf@zu.edu.eg
* Correspondence: a_ashraf@zu.edu.eg; Tel.: +20-1005-237-673

Abstract: As V2X technology develops, acute problems related to reliable and secure information exchange between network objects in real time appear. The article aims to solve the scientific problem of building a 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 authors present a formalized mathematical model of the system, taking into account the interconnection of objects and V2X information channels, and an energy-efficient algorithm of traffic offloading to the MEC server. The paper presents the results of application of blockchain technologies and mobile edge computing in the developed system, their description, evaluation of advantages and disadvantages of the implementation.

Keywords: vehicular network; VANET; vehicle-to-everything; mobile edge computing; blockchain; blockchain sharding

1. Introduction

The broad attention of the global community to the 2030 networks has made a significant contribution to the development of many new and improved existing technological and technical capabilities. One of the leading objects of research in these networks was the transportation system in the context of unmanned driving, automated transport and driver assistance services [1].

As a consequence, vehicle-to-everything (V2X) technology has gained enormous interest from leading powers, vehicle manufacturers, research and scientific communities and committees [2]. The development of this sphere will increase the safety of road users, improve traffic flow and, consequently, reduce the negative impact on the environment.

As V2X technology evolves, there are acute challenges associated with reliable and secure real-time information exchange between network objects. These challenges are complicated by the high mobility of much of the V2X infrastructure, such as cars, cyclists and pedestrians. It is also worth considering the large number of heterogeneous network participants at certain intervals. Thus, V2X can be divided into four main types: vehicle-network interaction (V2N), vehicle-to-vehicle interaction (V2V), vehicle-infrastructure interaction (V2I), vehicle-human interaction (V2P) [3]. At the same time, the lack of trust between the objects of the transport network can negatively affect the activities

and interaction, as well as lead to casualties, privacy violations and other irreversible consequences. In order to ensure the quality of services and reduce the negative effects of the influence of unscrupulous participants in the transport interaction, the authors propose the use of blockchain at the level of exchange participants and RSUs.

The development of such networks is a prerequisite for improving the dynamic requirements for 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 [4]. To provide and support the given service requirements, mobile edge computing (MEC)-based task offloading will be effective in some cases.

However, when performing MEC-based compute offloading, malicious service providers can cause serious security problems, which hinders the widespread adoption of this solution. To solve this problem, a scheme using blockchain technology based on smart contracts between service providers and mobile peripheral computing devices is proposed.

Motivated by the described state-of-the-art technology, this paper first explores the problem of building a network architecture to reliably deliver correct and uncompromised data in a Vehicle for Everything (V2X) framework to improve road user safety using blockchain technology and mobile edge computing (MEC).

Motivated by the described state-of-art, this work studies the problem of constructing a network architecture for reliable delivery of correct and non-compromised data within the framework of the vehicle-to-everything (V2X) concept to improve the safety of road users, using blockchain technology and mobile boundary computing (MEC).

V2X technology involves complex, multi-faceted systems that address traffic safety, traffic management efficiency, and driving comfort. To achieve these goals, V2X technology must provide 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 amounts of data. This paper aims at solving fundamental problems, which are of fundamental importance for creating an effective basis in the implementation of V2X technology.

Our novel contributions can be summarized as follows:

1. We analyzed the indicators of reliability, sustainability, QoS and resource provision of infrastructure facilities in particular and the V2X system in general.
2. We proposed 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. We aim to create a complex mathematical model of the system, taking into account the interconnection of objects and channels for V2X information transmission.
4. We include a system model and performed simulations that prove that our proposed model is effective in practical vehicle networks.

To solve the problems the following methods and approaches will be used: principles and methods of system analysis, heuristic search, methods of optimization and algorithmization, logical-structural, structural-parametric and comparative analysis, mathematical statistics. Methods of analytical and simulation modeling.

The rest of the article is structured as follows: Section 3, we summarize the main features of our proposal for the system architecture, taking into account the integration of blockchain technologies, and the resulting mathematical model is presented in Section 4. The obtained results are analyzed in Section 5. Finally, the conclusions and future work are presented in Section 6.

2. Related Works

A large number of researchers put the provision of data security and integrity, provision of high QoS scores and resource saving as the most important tasks for 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 following studies can be highlighted, which allow us to assess the importance of considering this problem.

Many researchers, for example, [5] consider the problems associated with the implementation of projects to improve the transport infrastructure, and include various solutions to improve management, as well as describe 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 in computing tasks in the network leads to repeated packet transmissions, which increases the energy consumption. In a study [6], 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 [7], in order to reduce the execution delay and computational energy consumption, a MEC system with multiple independent tasks of joint scheduling offload optimization and transmission power allocation was proposed. A study [2] 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 tradeoff between deployment cost and latency, with latency-tolerant services generally placed in the core of the cloud to reduce cost, while latency-critical services were placed at the edge to maintain their QoS requirements. In [8], 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 [9] 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 [10]. To reduce the overhead of a V2X network, a problem is proposed in which the optimal offload solution, transmission power management, sub-channel assignment, and computational resource allocation scheme are given. The offloading solution is modeled as a potential game, and the Nash equilibrium is confirmed by constructing a potential function.

In [11], common V2X threats are discussed and existing V2X authentication solutions are considered, while pointing out the importance of blockchain solutions in the field of critical data security for the presented networks. In [3] 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, an experiment that showed the numerical characteristics of resource allocation on the devices involved in the organization of V2N communication, is proposed. In [12], the authors proposed a blockchain-based secure computing offloading scheme in the vehicle-to-network cloud, which includes a blockchain-based trust management and a smart contract based on the DRL algorithm. In [13], the authors proposed a trust model to calculate each neighbor's trust value and used the trust value to decide whether or not to accept a data message from a neighbor. In [14–16], 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

and make an assessment of the relevance of the technology in the field of data security and reliability.

In the study [17], the authors include an additional security mechanism based on an information-oriented evaluation of the reliability of the received danger messages. The study [18] considers different characteristics of DLT technology and concludes that the 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 [19], the authors propose a new type of local blockchain to solve critical message propagation problems in V2X/VANET. Evaluation and analysis 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, as well as most studies do not consider approaches to the choice of consensus algorithm 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 implies a 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 varying and predicting system parameters and costs for different tasks and requirements, which is of significant importance in the implementation and use of V2X technology.

A significant number of publications of scientists from different universities and corporations on the main directions of the project confirm 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.

3. V2X system architecture when integrating blockchain technology and MEC

The proposed system architecture consists of roadside participants, several RSUs, as well as MECs and cloud servers, the architecture is shown in Figure 1.

Roadside Unit (RSU). RSUs are used to link services to V2X objects moving on/around the road and provide route information and updates. V2X System Participant Devices. This device is used to periodically transmit and request traffic-related information. Participants can be vehicles, pedestrians, cyclists and others.

Mobile Edge Computing (MEC) and cloud services. To deploy the proposed architecture, the network must be equipped with edge servers connected with high bandwidth.

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 require new road network planning [20].

Thus, it should be noted, 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.

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.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 December 2021 doi:10.20944/preprints202112.0204.v1

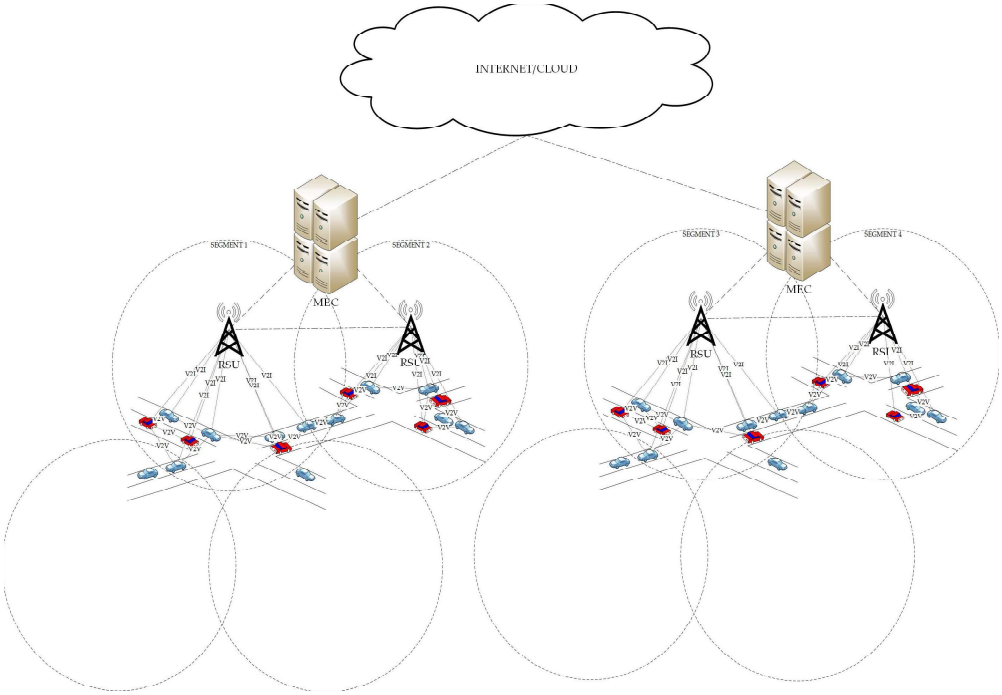

Figure 1. The architecture of the proposed system

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 [21,22] and detailed service requirements, which are shown in Table 1.

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 and so on.

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 will be subjected to cyber-attacks targeting vehicular communications [23]. 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

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 will 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 will allow action to be taken against offenders and encourage decent users. This will 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 will 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, 2 parameters will be used in messaging, first the event information itself, the second the priority of the message based on the service category and on the reputation of the object (rep). This method will allow a more objective perception of the real situation, 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 Practical Byzantine Fault Tolerance (PBFT) consensus algorithm, which is responsible for efficient operation in asynchronous networks, allows reaching consensus even if some nodes in the network do not respond or give wrong information. This algorithm involves selecting 2 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 new 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.

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, data is 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 their 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, until the device is considered an intruder until the reasons are clarified. If, however, 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, 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

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 December 2021 doi:10.20944/preprints202112.0204.v1

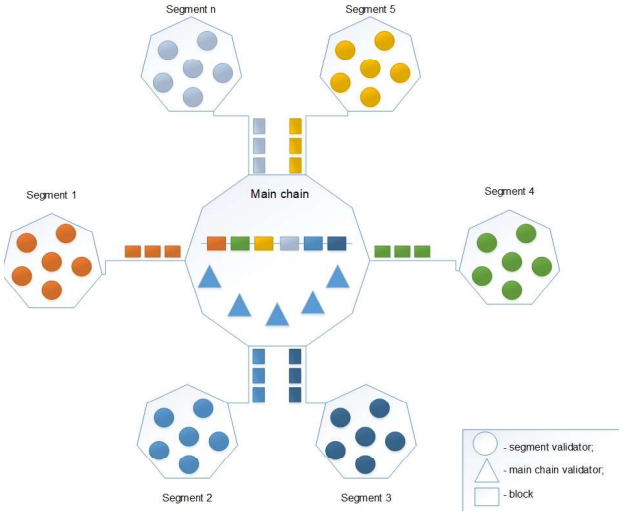

Figure 2. Multi-chain architecture

round for transactions with coefficient (k) below 0.6, 2/4 for transactions with coefficient (k) above or equal to 0.6.

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

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 [24].

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 [25]. 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 number of nodes and block generation times. The Chameleon, Omniledger [26], or Elastico [27] 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 is stored in a complete chain of a certain period of time, for example, one day or one week, and the previous blocks will be stored in multi-chains. It is worth noting that a segmented system model must account for the negligible probability that any segment will be compromised.

The authors also do not deny that in the future a Cosmos Network-type protocol could be used instead of segmentation [28], but at the time of writing these types of solutions were only in the development stage and have no final solution.

If we consider the procedure of selecting the entry and exit of the segment, it should be noted 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.

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 [29]. To solve these problems, the European Telecommunications Standards Institute in 2014 proposed the use of mobile peripheral computing [2]. 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 that can lead to accidents [22]. In addition to this, the devices additionally require additional services, such as computing and updating the user rating and network segment selection, which is a very time-consuming process, and it also 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 RSU load is high, the 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 MECs 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 the 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.

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, the 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, 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 Fig. 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 need 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[1] which can provide the computation and storage capabilities for vehicles. Moreover, in this plane, we configure 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 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 computing servers set that are utilized to process the vehicles' task, in which 0 denotes that the task will be

[1] RSUs and edge servers are interchangeably used in this paper.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 December 2021 doi:10.20944/preprints202112.0204.v1

processed locally at vehicle itself and and $N+1$ denotes that the task will be processed at cloud server. In addition, $\alpha_{i,j} \in \{0,1\}$ is used to denote the decision of offloading for vehicles' task, in which ($\alpha_{i,0} = 1$) and ($\alpha_{i,N+1} = 1$) mean that the task will be processed locally and remotely at cloud server, respectively. Whereas, ($\alpha_{i,j} = 1, \forall_j \in [1..N]$) means that the vehicles' task will 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 [30,31], 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 V2X networks problem.

3.4.1. Communication Model

This subsection will start with an introduction to the model of communication, where the system environment is respectively composed of a $\mathbb{B}$ and $\mathbb{A}$ sets of RSUs and vehicles. 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 cycles' number of CPU demanded to complete the computation task. Guided by the work in [32,33], a_i and c_i' values can be obtained through the task execution profiling.

Regrading the intuition shown in [34], in this study, we chose to disregard the consumption overhead in terms of time and energy for transmitting the result back to vehicles, since the output data are small relative to the input data.

Note that, in the case of multi vehicles transmissions in the same cell, orthogonal frequency-division multiplexing method is utilized to mitigate the intracellular interference[34,35]. In addition, according to Shannon law[36], the uplink data rate for the 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 of vehicle i, 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 $\mathbb{A}$ set of vehicles that are connected a $\mathbb{B}$ set of RSUs via wireless channel. Additionally, each vehicle i has an intensive task for being processed locally at vehicle or preserved as 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, will be discussed in the next subsections.

Local Execution Approach

Local execution approach takes into account that different vehicles may have different capabilities of computation. Moreover, each vehicle will 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:

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

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

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 $/vartheta_i$.

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 edge or cloud servers can be computed accordingly:

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

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

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

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

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

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 Eqs.(3, 4, 8, 9), and 10, the total time and energy for performing all the computation task 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 investigate 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:

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 December 2021 doi:10.20944/preprints202112.0204.v1

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

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, respectively, addressed through the first two constraints (i.e., C1 and C2). Whereas, the execution limit (i.e., only one time) for each vehicle's i task is guaranteed via constraint C3. Finally, the binarization of 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 decision offloading variables α^*. Therefore, branch and bound technique is used in this study in accordance with [37,38] to solve this problem.

3.5.1. 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 Eq.(13), the core newtork can derive the optimal offloading decision for each vehicle's task through problem solution. Finally, each RSU send the offloading decision for each vehicle which determines wherever the task will be executed (i.e., locally, edge or cloud server). The detailed process for energy-efficient task offloading is outlined in Algorithm 1.

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 Eq.(13).
9: Send the offloading decision values to each vehicle i.

4. Performance Evaluation

In this part, the developed blockchain-MEC V2X system is evaluated over the NS-3 platform. Table 1 provides the considered simulation parameters. There are seven MEC servers considered for the simulation process, with the specifications introduced in Table 1. Vehicles are located randomly, with the specifications introduced in Table 1. Each vehicle is assigned a workload equivalent to the workload of real tasks. The number of deployed vehicles, N, is assigned three values, as the system is simulated for 200, 400, and 600 vehicles to check the effect of the traffic increase on the performance of

 doi:10.20944/preprints202112.0204.v1

the developed blockchain-MEC V2X system. Moreover, three densities of vehicles are considered for the simulation process to evaluate the effect of the change of vehicle density, TD, on the overall system performance.

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

Table 1. Simulation parameters.

Parameter	Value
No. of vehicles (N)	$200, 400, 600$
Number of MEC units	7
Density of vehicles (TD)	$0.1, 0.2, 0.3\ veh/m$
MEC placement	*equidistant*
Streaming service bandwidth	$[10, 2048]\ (Kb/S)$
Vehicle task energy	$[20, 80]\ (watt/sec)$
Transmit power	$13\ dB$
Storage / RAM	$2048\ Mb$
Storage/HDD	$5\ Gb$
Processing / CPU	$[0.7, 2.5]\ GHz$

Figure 3, presents the percentage of the communication overhead for system (II) compared to system (I), for a three different cases of traffic density. As the traffic density increases, the communication overhead increases by an average of 13% per each 10% of traffic density increase. Furthermore, clustering reduces the communication overhead of the developed blockchain-MEC V2X system; however, when the percentage of cluster-heads (leader nodes) reaches 70% of all vehicles in the cluster, the clustering is no more efficient, and the communication overhead is 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 increase in the network, the average communication overhead increases. Moreover, to evaluate the effect of the vehicle mobility on the developed blockchain-MEC V2X, the communication overhead is measured for different values of vehicle mobility. Figure 5 presents the communication overhead of system (II), compared to system (I), with the change of the vehicle mobility; at a cluster-head percentages of 10, 20, and 30 from the total number of cluster members. The communication overhead increases linearly till a mobility of 60 km/h., then the increase of vehicle mobility produces a higher increase of the communication overhead.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 December 2021 doi:10.20944/preprints202112.0204.v1

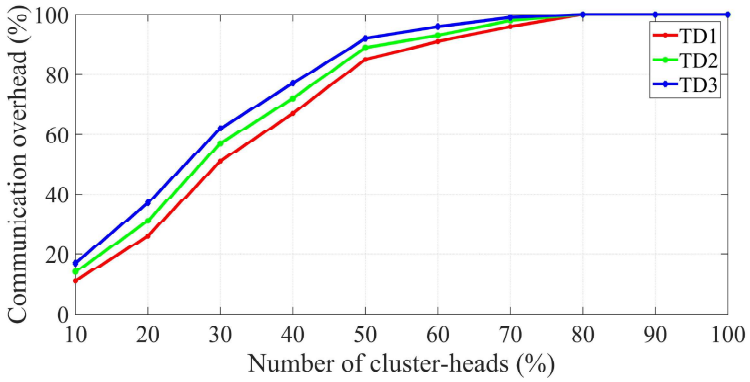

Figure 3. Percentage of the communication overhead with the change of the number of cluster-heads, for different values of traffic density.

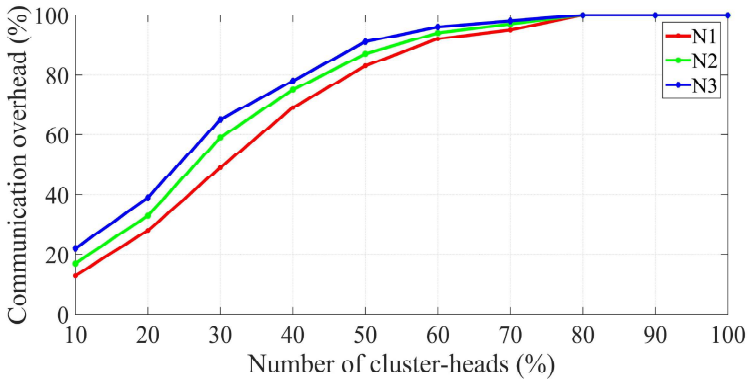

Figure 4. Percentage of the communication overhead with the change of the number of cluster-heads, for different values of number of deployed vehicles.

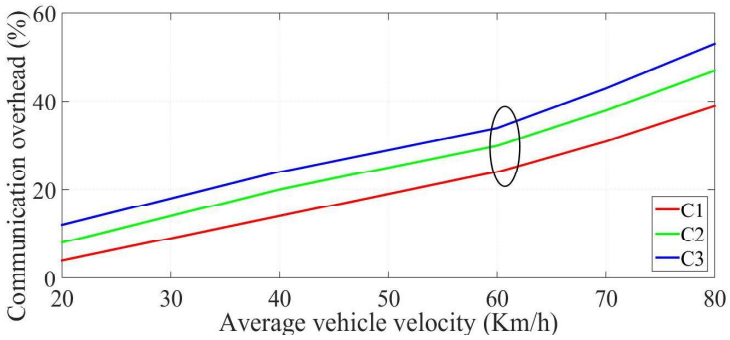

Figure 5. Percentage of the communication overhead with the change of the vehicle velocity.

The percentage of blocked tasks compared to total number of computing tasks is 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 three considered cases, at 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) is introduced for the developed system with the optimized offloading scheme. The optimized offloading scheme achieves the highest performance of task handling, even with the increase of the number of vehicles. Figure 7 provides the average percentage improvement of

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 December 2021 doi:10.20944/preprints202112.0204.v1

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 achieves an average improvement of the latency performance of 39% compared with the traditional systems. The developed offloading scheme with the blockchain-MEC V2X improves the energy efficiency of the system by reducing the energy consumption of the 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 achieves an average improvement of energy efficiency of 36% compared to the traditional V2X systems.

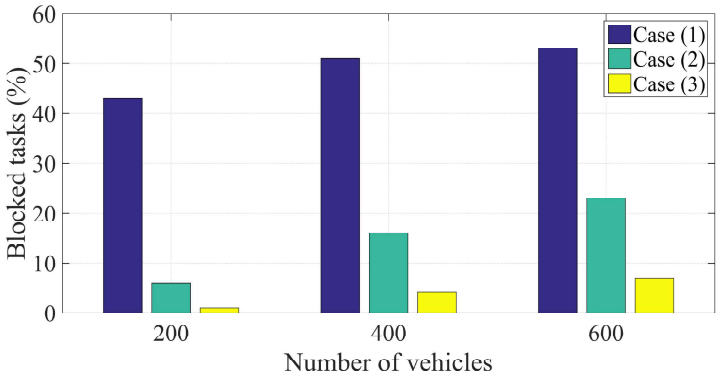

Figure 6. Average percentage of blocked tasks at different values of deployed vehicles.

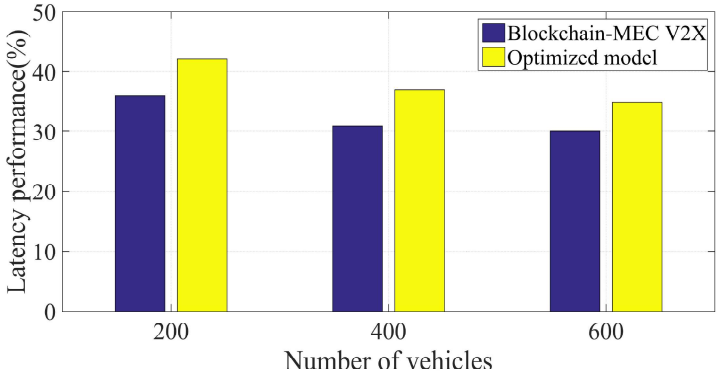

Figure 7. Latency performance of the developed systems compared with the traditional systems, for different values of deployed vehicles.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 13 December 2021 doi:10.20944/preprints202112.0204.v1

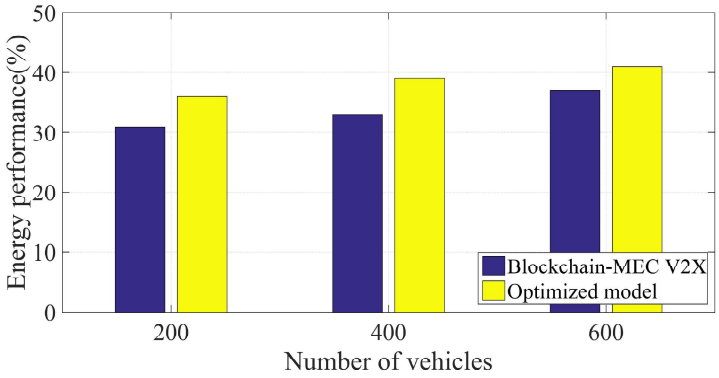

Figure 8. Energy performance of the developed systems compared with the traditional systems, for different values of deployed vehicles.

5. Discussion

The developed blockchain-MEC V2X system achieves higher reliability tan existing V2X models. The optimized blockchain-MEC v2x reduces the percentage of blocked tasks by an average of 41% compared to traditional v2x system. 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 the latency efficiency. The optimized model of the developed system achieves an improvement of average latency efficiency of 39% compared to traditional systems. The introduction of MEC servers reduces the communication latency, and with the optimized offloading scheme the resources are utilized in a higher efficient way that achieves this latency performance improvement. Furthermore, the optimized model of the developed v2x system achieves higher energy efficiency than traditional systems, by an average of 36%. This is due to task offloading, which is performed in an optimized way that achieves the minimum energy consumption in handling each task.

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 is introduced in a way that achieves the required level of security. RSUs are connected with edge computing servers that is integrated with the introduced blockchain model. A computational offloading scheme has been developed and introduced in a way that reduces the latency in handling computing tasks. The model has been optimized in terms of energy to reduce the over all energy consumption. The developed blockchain-MEC model has been evaluated over NS-3 environment for various simulation scenarios, and results validate the system in terms of reliability, latency, and energy efficiency. The optimized model of the developed system achieves higher latency efficiency of 39%, and higher energy efficiency of 36% than traditional v2x systems.

Author Contributions: Conceptualization, A.V., A.A.A. and A.M.; methodology, A.V., A.K. 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., N.V. and A.M.; visualization, A.V. and A.S.; supervision, A.V. and A.A.A.; project administration, A.M.; funding acquisition, V.E.

Funding: Research funded by Ministry of Digital Development, Communications and Mass Media of the Russian Federation, contract number 33-1-26/9 (Moscow, Russia).

Acknowledgments: The researcher A.A. Ateya is 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 preprint arXiv:2103.14225* **2021**.
2. Moubayed, A.; Shami, A.; Heidari, P.; Larabi, A.; Brunner, R. Cost-optimal v2x service placement in distributed cloud/edge environment. 2020 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)(50308). IEEE, 2020, pp. 1–6.
3. Muthanna, A.; Shamilova, R.; Ateya, A.A.; Paramonov, A.; Hammoudeh, M. A mobile edge computing/software-defined networking-enabled architecture for vehicular networks. *Internet Technology Letters* **2020**, *3*, e109.
4. Mei, J.; Wang, X.; Zheng, K. Intelligent network slicing for V2X services toward 5G. *IEEE Network* **2019**, *33*, 196–204.
5. Nellore, K.; Hancke, G.P. Traffic management for emergency vehicle priority based on visual sensing. *Sensors* **2016**, *16*, 1892.
6. 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 Vehicular Technology Magazine* **2017**, *12*, 36–44.
7. Mao, Y.; Zhang, J.; Letaief, K.B. Joint task offloading scheduling and transmit power allocation for mobile-edge computing systems. 2017 IEEE wireless communications and networking conference (WCNC). IEEE, 2017, pp. 1–6.
8. 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.
9. Shrestha, R.; Nam, S.Y.; Bajracharya, R.; Kim, S. Evolution of V2X Communication and Integration of Blockchain for Security Enhancements. *Electronics* **2020**, *9*, 1338.
10. Zhang, H.; Wang, Z.; Liu, K. V2X offloading and resource allocation in SDN-assisted MEC-based vehicular networks. *China Communications* **2020**, *17*, 266–283.
11. Muhammad, M.; Safdar, G.A. Survey on existing authentication issues for cellular-assisted V2X communication. *Vehicular Communications* **2018**, *12*, 50–65.
12. Xu, S.; Guo, C.; Hu, R.Q.; Qian, Y. BlockChain Inspired Secure Computation Offloading in a Vehicular Cloud Network. *IEEE Internet of Things Journal* **2021**.
13. Liao, C.; Chang, J.; Lee, I.; Venkatasubramanian, K.K. A trust model for vehicular network-based incident reports. 2013 IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC). IEEE, 2013, pp. 1–5.
14. Vladyko, A.; Spirkina, A.; Elagin, V. Towards Practical Applications in Modeling Blockchain System. *Future Internet* **2021**, *13*, 125.
15. 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.
16. Elagin, V.; Spirkina, A.; Buinevich, M.; Vladyko, A. Technological aspects of blockchain application for vehicle-to-network. *Information* **2020**, *11*, 465.
17. Ostermaier, B.; Dotzer, F.; Strassberger, M. Enhancing the security of local dangerwarnings in vanets-a simulative analysis of voting schemes. The Second International Conference on Availability, Reliability and Security (ARES'07). IEEE, 2007, pp. 422–431.
18. Kannengießer, N.; Lins, S.; Dehling, T.; Sunyaev, A. Mind the gap: trade-offs between Distributed Ledger Technology characteristics. *arXiv preprint arXiv:1906.00861* **2019**.
19. Shrestha, R.; Bajracharya, R.; Shrestha, A.P.; Nam, S.Y. A new type of blockchain for secure message exchange in VANET. *Digital communications and networks* **2020**, *6*, 177–186.
20. Sharma, P.K.; Moon, S.Y.; Park, J.H. Block-VN: A distributed blockchain based vehicular network architecture in smart city. *Journal of information processing systems* **2017**, *13*, 184–195.
21. Campolo, C.; Molinaro, A.; Iera, A.; Menichella, F. 5G network slicing for vehicle-to-everything services. *IEEE Wireless Communications* **2017**, *24*, 38–45.
22. Islam, S.; Badsha, S.; Sengupta, S.; La, H.; Khalil, I.; Atiquzzaman, M. Blockchain-Enabled Intelligent Vehicular Edge Computing. *IEEE Network* **2021**, *35*, 125–131.
23. El-Rewini, Z.; Sadatsharan, K.; Selvaraj, D.F.; Plathottam, S.J.; Ranganathan, P. Cybersecurity challenges in vehicular communications. *Vehicular Communications* **2020**, *23*, 100214.
24. Yu, Y.; Liang, R.; Xu, J. A scalable and extensible blockchain architecture. 2018 IEEE International Conference on Data Mining Workshops (ICDMW). IEEE, 2018, pp. 161–163.
25. Aiyar, K.; Halgamuge, M.N.; Mohammad, A. Probability distribution model to analyze the trade-off between scalability and security of sharding-based blockchain networks. 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC). IEEE, 2021, pp. 1–6.
26. He, G.; Su, W.; Gao, S. Chameleon: a scalable and adaptive permissioned blockchain architecture. 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018, pp. 87–93.
27. Luu, L.; Narayanan, V.; Zheng, C.; Baweja, K.; Gilbert, S.; Saxena, P. A secure sharding protocol for open blockchains. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 17–30.
28. 28. Cosmos. Interchain Standards. https://github.com/cosmos/ibc, accessed on 17.10.2021.
29. Li, D.; Xu, S.; Li, P. Deep reinforcement learning-empowered resource allocation for mobile edge computing in cellular v2x networks. *Sensors* **2021**, *21*, 372.
30. Zhao, Z.; Guardalben, L.; Karimzadeh, M.; Silva, J.; Braun, T.; Sargento, S. Mobility prediction-assisted over-the-top edge prefetching for hierarchical VANETs. *IEEE Journal on Selected Areas in Communications* **2018**, *36*, 1786–1801.

31. Yao, L.; Chen, A.; Deng, J.; Wang, J.; Wu, G. A cooperative caching scheme based on mobility prediction in vehicular content centric networks. *IEEE Transactions on Vehicular Technology* **2017**, *67*, 5435–5444.
32. Lyu, X.; Tian, H. Adaptive receding horizon offloading strategy under dynamic environment. *IEEE Communications Letters* **2016**, *20*, 878–881.
33. Liu, F.; Huang, Z.; Wang, L. Energy-efficient collaborative task computation offloading in cloud-assisted edge computing for IoT sensors. *Sensors* **2019**, *19*, 1105.
34. Elgendy, I.A.; Zhang, W.; Tian, Y.C.; Li, K. Resource allocation and computation offloading with data security for mobile edge computing. *Future Generation Computer Systems* **2019**, *100*, 531–541.
35. Deb, S.; Monogioudis, P. Learning-based uplink interference management in 4G LTE cellular systems. *IEEE/ACM Transactions on Networking (TON)* **2015**, *23*, 398–411.
36. Chatzinotas, S.; Imran, M.A.; Hoshyar, R. On the multicell processing capacity of the cellular MIMO uplink channel in correlated Rayleigh fading environment. *IEEE Transactions on Wireless communications* **2009**, *8*, 3704–3715.
37. 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.
38. 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 of Things Journal* **2020**, *8*, 8119–8132.