applied sciences

MDPI

Article

VaNetChain: A Framework for Trustworthy Exchanges of Information in VANETs Based on Blockchain and a Virtualization Layer

Paúl Vintimilla-Tapia [1,*], Jack Bravo-Torres [1,*], Martín López-Nores [2], Pablo Gallegos-Segovia [3], Esteban Ordóñez-Morales [1] and Manuel Ramos-Cabrer [2]

[1] Grupo de Investigación en Telecomunicaciones y Telemática (GITEL), Universidad Politécnica Salesiana, 010102 Cuenca, Ecuador; eordonez@ups.edu.ec

[2] AtlantTIC Research Center, University of Vigo, 36310 Vigo, Spain; mlnores@det.uvigo.es (M.L.-N.); mramos@det.uvigo.es (M.R.-C.)

[3] Grupo de Investigación en Cloud Computing, Smart Cities & High Performance Computing (GIHP4C), Universidad Politécnica Salesiana, 010102 Cuenca, Ecuador; pgallegos@ups.edu.ec

* Correspondence: pvintimilla@ups.edu.ec (P.V.-T.); jbravo@ups.edu.ec (J.B.-T.); Tel.: +593-99-805-7994 (P.V.-T.)

Received: 28 September 2020; Accepted: 2 November 2020; Published: 9 November 2020

check for updates

Featured Application: A framework to enable data integrity, traceability and reliability in the information exchanges between vehicles and roadside units, relying on blockchain technology and a virtualization layer.

Abstract: Vehicular ad hoc networks (VANETs) face challenges related to the reliability of the data exchanged and the unstability of the communication links. These shortcomings have hampered the development of the long-awaited applications that would turn roads into a smart environment. We present a framework to deploy such services, in which a virtualization layer ensures means to efficiently deliver messages between vehicles and roadside units (RSUs) and, on top of that, blockchain technology is used to enable features of data integrity, traceability, and reliability that cannot be furnished by existing consensus and reputation mechanisms. A simulation experiment is included to determine the optimal number of RSUs to be installed as supporting infrastructure in a city.

Keywords: vehicular ad-hoc network; virtualization; blockchain; reliable data; vehicular crowdsensing

1. Introduction

The automotive industry is undergoing a revolution, driven by the advances in information and communication technologies and microelectronics, towards the deployment of intelligent transportation systems [1,2]. Vehicular ad hoc networks (VANETs) are highly dynamic and self-organizing networks, formed by vehicles equipped with on-board units (OBUs) for direct short-range communications (DSRC) with other vehicles and roadside units (RSUs) [3]. DSRC standards were recently adopted by the European Parliament—to the detriment of the alternative model of cellular vehicle-to-everything (C-V2X) [4]—to enable specific solutions for increased road safety, traffic efficiency, driving assistance, crowdsensing, infotainment, and many others [5–17].

Managing the information required by these new services often goes beyond the capabilities and/or the incumbency of individual vehicles, e.g., because the amount of data exceeds the memory and CPU power of the OBUs, because a peer-to-peer model is not suitable for a given task, or due to privacy concerns. For example, in dealing with traffic accidents, insurance companies use as much information as possible about the circumstances to determine responsibilities and execute the contracts.

Thus, they are interested in gathering telemetry data sensed by nearby nodes in the VANET, which they can consolidate and analyze in the cloud, and thereupon make the decision of whether to pay for the damages [18]. In general, it is necessary to create solutions in which the vehicles can collaborate to effectively augment their capabilities, by sharing processing/storage/sensing resources with other vehicles and establishing reliable communication paths to fixed RSUs, which may act as gateways to the Internet [19,20] or carry out some processing in an *edge computing* fashion [21,22].

For the new services to work properly, it is necessary to address two challenges inherent to the vehicular environment: the instability of the communication links and the trustworthiness of the data generated/provided by the vehicles [23]. On the one hand, the rapid mobility and the variations of vehicle density lead to breakages of the communication links between pairs of vehicles, affecting any multi-hop communication paths established through them [19,24]. On the other hand, due to the nature and sensitivity of the information exchanged in some services (e.g., geographic locations, license plates or any other form of identity, etc.), there must be ways to prevent or hamper malicious behavior, dealing at least with data integrity and traceability, and assessing the reliability of the data sources according to consensus and reputation mechanisms [25–28]. The notions of information quality and criticality described in [29] emerge, too, in order to quantify the importance level of the information that each source may contribute.

In this paper, we present a framework that enables the desired VANET services by combining two technologies:

- First, a virtualization layer sits on top of the TCP/IP protocol stack to have the vehicles emulate a reliable network of static virtual nodes for the communications. In particular, we use the VaNetLayer system [30], which has been shown to improve the performance of VANET communications in simulations of urban scenarios [31].
- Second, blockchain technology is used to enable features of data integrity, traceability, and reliability that cannot be furnished by the consensus and reputation mechanisms that have shown up in the literature of VANETs in recent years. Specifically, we adopt the principles of Ethereum because its widely supported implementation of *smart contracts* provides suitable means for the definition of a range of service conditions.

In our framework, called the VaNetChain, the entwining of these technologies turns the RSUs into entities responsible for executing an improved consensus and validation protocol. In turn, the virtual nodes give maximum priority to the packets that imply adding/verifying information to/from the blockchain. Besides, they perform a pre-validation of the reputation of the vehicles involved in any exchange of messages, avoiding the propagation of false data and the waste of resources in the VANET.

The paper is organized as follows. Section 2 provides an overview of the state-of-the-art in routing protocols that attempt to reduce link breakages in VANETs, as well as previous approaches to improving the management of data in this context. Section 3 explains the architecture and the operating principles of the VaNetChain, focusing on the entwining between the VaNetLayer and blockchain technology. Section 4 presents an experiment aimed at determining the number of RSUs needed as fixed infrastructure in a city, focusing on latencies as a critical performance parameter. Finally, Section 5 contains conclusions and future work.

2. Related Work

The problems that the VaNetChain seeks to solve have been studied in the literature. On the one hand, a number of routing protocols have been designed and implemented to improve the stability of the communications in VANETs. On the other hand, several approaches have been proposed to enable reliable and traceable data exchanges against various types of defective or malicious behavior [32,33]. In the following subsections, we describe some of the most relevant works in relation to each topic.

2.1. Routing Protocols in VANETs

The dynamism, rapid mobility, and variable node densities that characterize the VANET environment hamper the collection and sharing of data, especially when high latencies are not tolerated [24]. Protocols based on geographic routing and clustering are currently seen as the most efficient choices, due to their efficient use of control messages. Geographic protocols use the nodes' positions to make routing decisions. Among the best known, IGRP [34] focused on selecting sequence of intersections for the packets to reach fixed gateway nodes (GWs). The GWs maintain an up-to-date view of the network topology. Therefore, every time a vehicle moves away from its current position a distance greater than its transmission range, it sends the nearby GWs a report with its updated location. This information allows the calculation of a set of routes to maximize the QoS parameters. An alternative approach was presented in [35], based on a data dissemination scheme to perform intelligent forwarding, by selecting the next hop according to the stability of the connection and the link durations.

In clustering-based protocols, the idea is to introduce a hierarchy to handle manageable amounts of control messages, by arranging the moving vehicles in groups (typically, on the grounds of geographical proximity and relative movement) and designating one of them as the cluster head to channel the communications with the neighboring groups. An interesting analysis of approaches to form clusters was presented in [36], while the work in [37] enumerated parameters relevant for the selection of the cluster heads. New combinations of approaches for both tasks keep appearing, achieving significant performance improvements in simulation experiments [38]. As the routing protocol between cluster heads, it is still common to find variations of classical algorithms—such as AODV or OLSR—to use the most reliable routes from source to destination. For example, in [39] the traditional system for the detection of route breakages (based on the loss of HELLO messages) was replaced by a forecasting indicator that used information about errors in the decoding of OFDM packets. The authors of [40], in turn, developed a framework that analyzes network resources in order to adjust the relationship between topology changes and QoS needs, aiming to decrease the load on the VANET and thereby improve scalability. Other authors have attained improvements by incorporating machine learning techniques that allow the prediction of vehicle mobility [41].

Finally, there are dedicated protocols running on the same idea of a layer of virtual nodes that supports the proposal in this paper, such as VNAODV+ [42] and VNIBR [43]. On the one hand, VNAODV+ maintains the reactive essence of AODV, including route discovery, packet types, and the configuration of most parameters. The main difference has to do with the changes required to send data through virtual nodes, starting from the fact that routing entities are not identified by IP addresses but by region. On the other hand, VNIBR is an intersection-based geographical protocol in which all routing decisions are made at road intersections, where the virtual nodes maintain routing tables as persistent state information.

2.2. Reliability and Traceability of Data in VANETs

As explained in [26], VANET communications may be affected by nodes that alter the content of the messages that they should simply relay, or that generate false data. Some authors have proposed trust models as a first facility to address this problem, which can be classified into three categories:

- Some approaches assess the reliability of the vehicles through a reputation system that relies on a centralized entity, which collects the opinions of neighboring nodes [44–47]. In scenarios of high mobility, these approaches struggle to collect sufficient information to calculate the reputation scores for each node; furthermore, the centralized entity represents a single point of failure.
- Other approaches resort to the cooperation among several sources of information to assess the reliability of the data they receive [48–50]. The need to replicate packets onto several nodes increases the communication overhead and the latencies, and in cases of high mobility it is hard to ensure the necessary levels of collaboration.

- Some proposals have combined the entity-centric and data-centric approaches, to jointly assess privacy and trust [51,52].

The literature of VANETs is rich in methods for authentication [53,54], including privacy-preserving techniques [55] which are highly needed for the kind of services advocated in this paper. On top of these, blockchain technology comes as a way to achieve traceability of the data, due to the introduction of a public, decentralized, hardly corruptible, and practically immutable ledger [56]. The recorded transactions, after being validated and added to the ledger, can be consulted at any time, but they cannot be deleted or modified [57]. The following are some remarkable proposals for the integration of blockchain in VANETs.

- The authors of [58] presented a reputation mechanism inspired by Bitcoin, in which unique cryptographic identifiers, known as the Intelligent Vehicle Trust Points (IV-TP), are created and delivered by authorized dealers. The higher the IV-TP achieved by a node, the more trustworthy it is considered.
- An anonymous blockchain-based reputation system was presented in [26], with two blockchains handled in parallel: the first one to store the certificates issued by a certification authority, together with the reputation scores of the corresponding nodes, and the second one to keep track of revoked public keys. When a communication is initiated between vehicles and/or roadside units, the validity of their certificates and public keys is checked by searching in the two blockchains. A similar approach was presented in [59], based on a lightweight blockchain protocol to keep track of all certificates (issued and revoked), whereas the authors of [60] made a proposal to speed up the authentication and revocation processes.
- The authors of [61] proposed a new type of blockchain to address aspects of security and reliability in the dissemination of emergency messages, which are relevant within a certain distance from the location of an incident. In order to validate the disseminated messages, the vehicles use certificates provided by the closest RSU, which guarantees that they were in a location close to the incident they are reporting.

In all of these approaches, the integration of blockchain in VANETs has been seen as a separate problem from the reliable transmission of data packets through one-hop or multi-hop routes. However, latencies and packet losses represent a persistent problem that cannot be diminished to an extent that does not impinge heavily on the performance of the blockchain protocols above [4]. Our approach to solve this inconvenience is to architecturally entwine a virtualization layer (which addresses the problems of the communications) and the blockchain protocol (which deals with the properties of the data). Our proposal is described in detail in the next section.

3. VaNetChain: Architecture

Figure 1 shows the difference between the protocol stacks of a traditional use of blockchain technology in VANETs and our proposal in this paper: VaNetChain. The key ideas of the latter are (i) to introduce the virtualization layer to support the operation of the routing algorithms (variations of the non-virtualized counterparts) and (ii) to entwine the operation of the blockchain protocols with the virtualization constructs.

The virtualization layer that supports our approach is called the VaNetLayer, introduced in [30] as an evolution of the VNLayer, a foundational proposal from the MIT [62]. The VaNetLayer defines procedures by which the moving vehicles collaborate to emulate fixed virtual nodes (VNs) that altogether cover the whole area of the VANET. The layout of the VNs is defined by first placing one VN at each intersection, and then covering the road segments with as many VNs as needed, depending on the maximum distance for one-hop communications. Figure 2 shows one example with 11 VNs, colored differently depending on whether they are covering one intersection, they are neighboring one intersection, or they are placed elsewhere on a road segment.

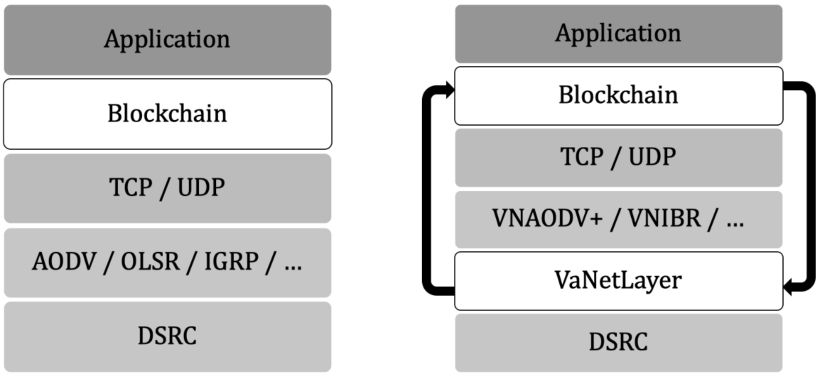

Figure 1. The protocol stack of previous uses of blockchain in vehicular ad hoc networks (VANETs) vs. the VaNetChain approach.

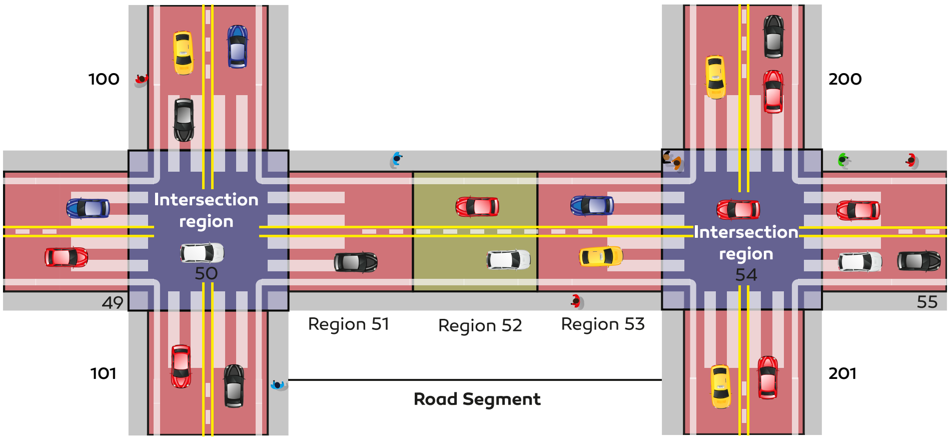

Figure 2. A sample deployment of virtual nodes with the VaNetLayer.

The emulation of the VNs is supported by one-hop communications among the vehicles that happen to be within the corresponding region at any given moment. These physical nodes can have three different roles: leader nodes, backup nodes, and regular nodes. As we will explain in Section 4, these roles are relevant at the blockchain level, too. Essentially, leaders are in charge of receiving/forwarding packets from/to neighboring VNs, as well as storing the persistent information state (PSI) kept in the region to support the operation of the protocols at higher layers. Backups, in turn, keep copies of the PSI as a mechanism to fight failures, and they support the leader's work in cases of intense traffic. Finally, the regular nodes listen to the dynamics of leader and backup appointments to replace them whenever needed.

At the blockchain layer, VaNetChain implements mining as a proof of work (PoW), designating RSUs as miners (mRSUs) that try to solve the block hash calculation by applying the Keccak (https://keccak.team/keccak.html) or SHA-3 algorithm. This idea goes hand in hand with the proposals that rely on RSUs to perform different computing tasks, taking advantage of computer and connectivity benefits [63]. The number of zeros required at the beginning of the hash is set so that an mRSU takes around 10 seconds to add a new block to the blockchain. If the time decreases for whichever reason, the number of zeros will increase accordingly, in order to ensure the immutability of the ledger. Likewise, if the time increases (e.g., due to periods of excessive work), mRSUs can choose to merge blocks of transactions and reduce the number of zeros in order to speed up things. The mRSUs set their gas limit ("gas" is the cost of making a transaction or executing a contract in Ethereum) to 1M. For the propagation of the new blocks (needed to achieve distributed consensus among the mRSUs and thus keep a unique record of transactions), the virtual nodes give the second greatest priority to the corresponding data packets —only second to the control packets of the VaNetLayer.

We assume that all VaNetChain participants can execute smart contracts and verify that their terms have been met. Reputation scores and a blacklist of MAC addresses are recorded in the blockchain along with the completed transactions. Thus, for any new transaction started by a vehicle (i.e., for any action to keep track of in the blockchain), the virtual node covering its current location can check its reputation and discard the transaction straight away if the value is too low or the vehicle has been blacklisted, thus helping to avoid waste of resources.

The behavior of the virtual nodes in VaNetChain has been extended with regard to the VaNetLayer in order to support the transient states while some transactions have not been added to the blockchain yet. This is summarized in the state diagram of Figure 3.

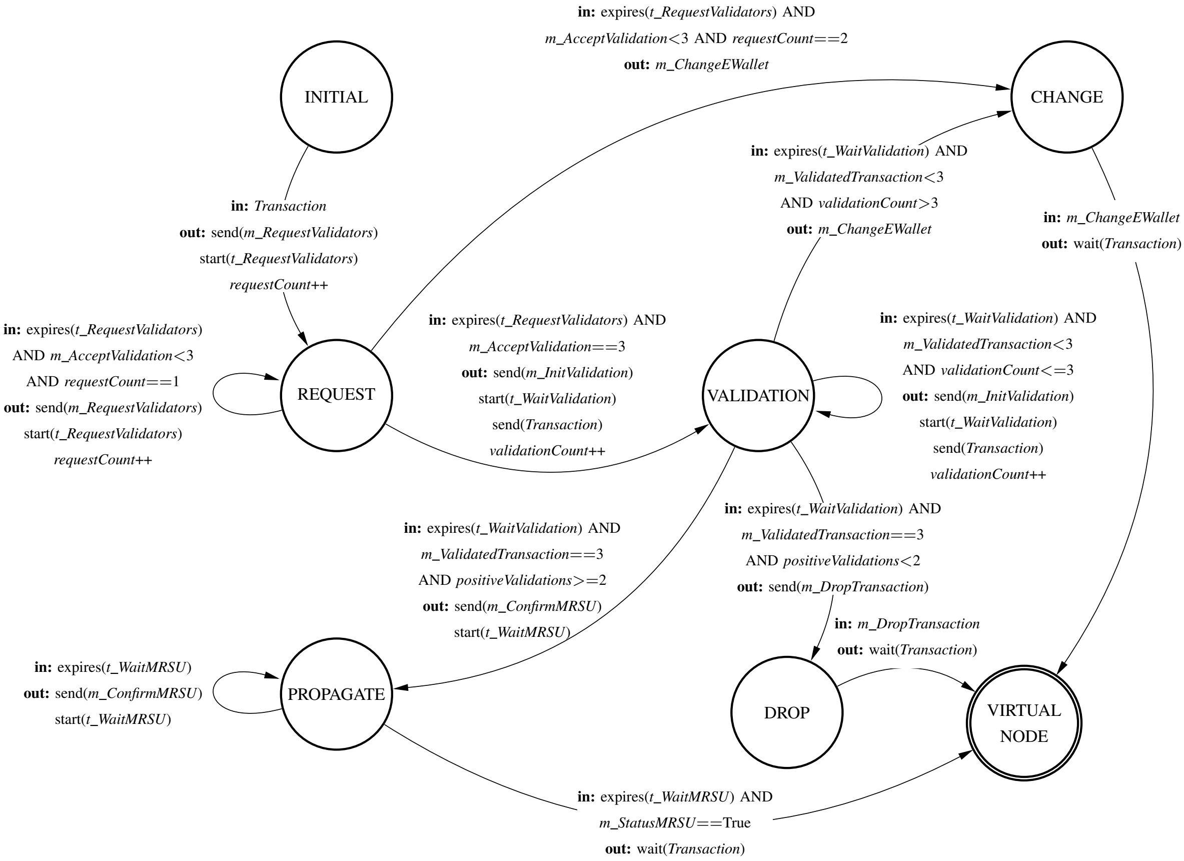
INITIAL
REQUEST
VALIDATION
CHANGE
PROPAGATE
DROP
VIRTUAL NODE
in: expires(t_RequestValidators) AND m_AcceptValidation<3 AND requestCount==2 out: m_ChangeEWallet
in: Transaction out: send(m_RequestValidators) start(t_RequestValidators) requestCount++
in: expires(t_RequestValidators) AND m_AcceptValidation<3 AND requestCount==1 out: send(m_RequestValidators) start(t_RequestValidators) requestCount++
in: expires(t_RequestValidators) AND m_AcceptValidation==3 out: send(m_InitValidation) start(t_WaitValidation) send(Transaction) validationCount++
in: expires(t_WaitValidation) AND m_ValidatedTransaction<3 AND validationCount>3 out: m_ChangeEWallet
in: m_ChangeEWallet out: wait(Transaction)
in: expires(t_WaitValidation) AND m_ValidatedTransaction<3 AND validationCount<=3 out: send(m_InitValidation) start(t_WaitValidation) send(Transaction) validationCount++
in: expires(t_WaitValidation) AND m_ValidatedTransaction==3 AND positiveValidations>=2 out: send(m_ConfirmMRSU) start(t_WaitMRSU)
in: expires(t_WaitValidation) AND m_ValidatedTransaction==3 AND positiveValidations<2 out: send(m_DropTransaction)
in: m_DropTransaction out: wait(Transaction)
in: expires(t_WaitMRSU) out: send(m_ConfirmMRSU) start(t_WaitMRSU)
in: expires(t_WaitMRSU) AND m_StatusMRSU==True out: wait(Transaction)

Figure 3. State machine of virtual nodes in relation to blockchain operations.

- In an INITIAL state, the VN waits for a physical node to initiate a transaction, which takes it to REQUEST state and sets to 0 the counters used thereafter: *requestCount* and *validationCount*.
- Within REQUEST, the *t_RequestValidators* timer is activated and an *m_RequestValidators* message is sent, incrementing the *requestCount* by 1. The objective is to request the presence of at least 3 local nodes in the region to pre-validate the transaction. If *t_RequestValidators* expires without reaching the minimum number of validators, the REQUEST is reactivated once, and if it fails again the VN evolves to CHANGE state. Otherwise, the state becomes VALIDATION.
- The CHANGE state denotes that the region does not have enough vehicles to pre-validate the transaction. In response to that, a neighboring VN is asked to take over by transmitting an *m_changeCVN* message.
- In VALIDATION state, the VN confirms the participation of the validators and responds with an *m_InitValidation* message, which activates the *t_WaitValidation* timer and increases the *validationCount*. This process is repeated up to 3 times, remaining in VALIDATION until it receives the requested verifications through *m_ValidatedTransactions* messages. If *validationCount* rises to 4, it automatically moves to CHANGE, otherwise it can fall into DROP or PROPAGATE.

- The DROP state means that positive validations were not sufficient, so the transaction is discarded. Then, an *m_DropTransaction* message is broadcast and the state becomes VIRTUAL NODE.
- Having got the minimum number of positive validations, the PROPAGATE state is reached, where the VN sends the validated transaction to the nearest mRSUS accompanied by the message *m_confirmMRSU*, which activates the *t_WaitMRSU* timer. While the timer is active, it waits for the confirmation message *m_StatusMRSU*==true. If this is not received, the process is repeated indefinitely in order to guarantee that the information has reached the mRSU.

4. Simulation Experiments

With the finished design of the VaNetChain, we proceeded to evaluate its performance through simulations under different conditions. In the specialized literature, there are no pre-established metrics on the use of blockchain in VANETs, as the diversity of uses, protocols, optimizations and cryptocurrencies prevent the standardization of parameters that could be considered optimal. Nonetheless, we could look at the consumption of gas in the Ethereum framework to assess the amount of work invested in the transactions. Prior to that, we analyzed the packet delivery ratios and the latencies incurred in the deployment of mRSUs, in order to understand the interrelationships between traffic densities, data volumes generated/transmitted in the VANET and fixed infrastructure needs.

4.1. Performance of the Communications

In the simulation experiments, we compared the latencies and the packet delivery ratios attained by three implementations of blockchain in VANETs:

- A non-virtualized configuration with a protocol stack like the one on the left hand side of Figure 1, with IGRP as the routing protocol.
- A VaNetChain configuration with a protocol stack like the one on the right hand side of Figure 1, with VNAODV+ as routing protocol (reactive).
- Another VaNetChain configuration with a protocol stack like the one on the right hand side of Figure 1, with VNIBR as routing protocol (geographic, intersection-based).

Latencies were measured as the time elapsed since a *m_ConfirmMRSU* message is sent until the *m_StatusMRSU* confirmation is received in the state machine of Figure 3. The consensus or mining time of a transaction is not part of this analysis, as the difficulty of the PoW is constantly adjusted to maintain a 10 seconds average.

The simulation scenario comprised a two-lane, 800 × 800 m Manhattan-type urban scenario with 64 intersections, 100 m away from one other. In the virtualized configurations, the road segments were always covered by 3 VNs (421 overall).

Regarding the simulation software, three tools were used: ns-3, 30th release (https://www.nsnam.org/releases/ns-3-30/), SUMO (https://sumo.dlr.de/docs/), and SimBlock (https://dsg-titech.github.io/simblock/). In ns-3, all the procedures followed by the VaNetLayer to achieve the emulation of VNs over PNs were defined; in addition, VaNetChain packets are given top priority thanks to the concept of cVN. SUMO is an urban mobility simulator that provides traces of node mobility. Finally, SimBlock is one good choice to implement a blockchain network, as its parameters can be modeled to model the behavior of any specific technology.

The parameters that are considered key to the simulations are summarized in Table 1.

In the first experiment, aiming to measure packet delivery ratios, we varied the vehicular density (128, 256 or 512 vehicles) in a scenario where 10,000 transactions had to be recorded. The results are shown in Figure 4. It can be seen that the VaNetLayer in conjunction with VNIBR yields the best results at low/medium density. The non-virtualized configuration with IGRP outperforms the virtualized one of VNAODV+, because the reactive nature of the latter fails to properly handle scenarios of high mobility. When comparing VNIBR and IGRP at high traffic densities, the differences are small differences because the mobility of the vehicles is reduced and, therefore, the environment is less challenging.

Table 1. The main parameters of our simulations.

Parameter	Value
Simulator	ns-3, SimBlock
Blockchain framework	Ethereum
Consensus algorithm	Proof of Work
Routing protocol	VNIBR-VNAODV+-IGRP
Simulation scenario	Manhattan type urban area
Propagation model	Hybrid buildings propagation loss model
Intersections number	64
Intersections separation	100 m
Number of PNs (vehicular density)	128-256-512
Number of VNs	421
mRSUs number	8-16-32
VaNetChain transactions	100-1000-10,000-100,000
VaNetChain packet size	1 MB
Transmission rate	6 Mbps
MAC	IEEE 802.11p
Transport protocol	UDP

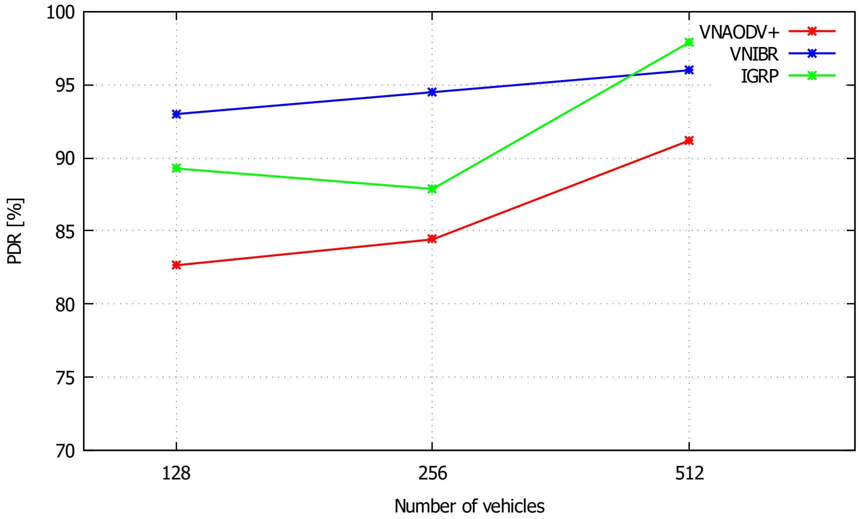

Figure 4. Packet delivery ratios measured against different numbers of vehicles in the VANET.

To assess end-to-end delays, we set the number of vehicles to 256 and progressively increased the number of transactions: 100, 1000, 10,000, and 100,000. The results can be seen in Figure 5. The curves of the three configurations exhibit similar dynamics, but VNIBR attains the best performance in all cases. VNAODV+ delivers packets more slowly, mainly because its route maintenance algorithms commonly lead to longer multi-hop paths. IGRP often makes the packets go through fewer hops, but it is less effective than VNIBR in dealing with route breakages, which causes retransmissions from the source and, thereby, additional delays.

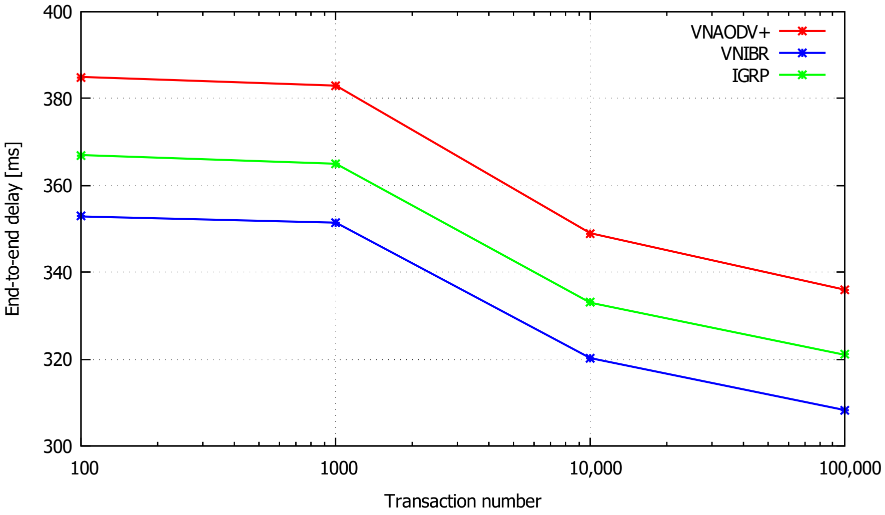

Figure 5. Latencies measured against different numbers of blockchain transactions.

Finally, because the mRSUs play a key role in mining and validating new blocks, we considered varying their number and checking how this affects the responsiveness of the VaNetChain. According to the criteria set out in [64], we found that the optimal number of mRSUs was 16; therefore, we changed it to 8 and 32 to establish a point of comparison. For this scenario, owing to the results of the previous experiments, VNIBR was established as a routing protocol. The vehicle density was set at 256 and the number of transactions was varied. The results are shown in Figure 6.

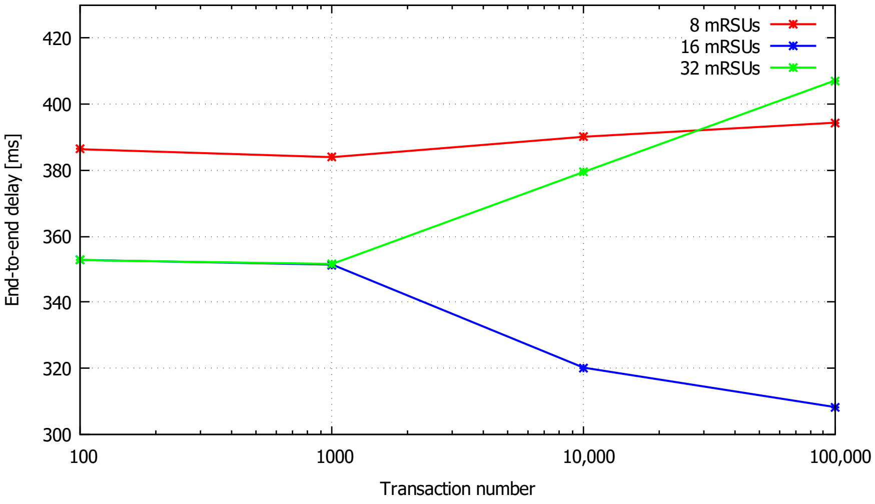

Figure 6. End-to-end delays measured with the VNIBR-based VaNetChain configuration in processing different numbers of transactions, with different numbers of mRSUS.

To begin with, it is interesting to note the stability shown by the curve corresponding to 8 mRSUs: although the number of transactions increases, the measured times range between 386 and 394 ms. The explanation lies in the fact that a lower density of mRSUs implies the participation of a greater number of virtual nodes in the transactions. Moreover, as the number of transactions increases, a small increase in the latency curve is due to the queuing caused by the pre-validation mechanisms.

When using 16 and 32 mRSUs, similar results were obtained up to 1000 transactions (around 350 ms), representing an improvement over 8 mRSUS, and therefore fewer virtual nodes involved in the retransmissions. From that point on, the delays with 16 mRSUs start to fall, reaching 308 ms with 100,000; in constrast, the delays increase progressively with 32 mRSUs, reaching 407 ms.

An excessive density of miners, therefore, can have a detrimental effect because it implies more mRSUs wasting resources in hash computation races won by others.

4.2. Cost of the Transactions

In order to assess the prospects for implementation in a real environment, we looked at the amount of gas involved in the execution of the intelligent contracts that support the VaNetChain. In Table 2, it can be noted that the valuation was the operation that entailed the greatest expenditure of gas, because it involves mathematical operations to calculate reputation based on the average of the responses. On the other hand, verifications and acceptances implied an average expense, due to the participation of at least three nodes to verify an event. Something similar happened with the blacklist operations, which incurred an average expense by adding a node and at the same time deleting it from the whitelist. Finally, the whitelist and the announcement operations caused the lowest expenses, as their execution only imply registering one variable.

Overall, the computational cost implied by these figures is not significant, given that Ethereum sets a limit of 8 M of gas [65] to avoid excessive expenses for the deployment of poorly-optimized contracts. This, added to the monetary values demanded in the different transactions (see Table 2), shows that the implementation of our proposal is feasible.

Table 2. Cost of intelligent contract execution (Gas price = 2 Gwei, 1 Ether = 395.02 USD, Date: October 2020).

Smart Contract	Gas Used	Actual Cost [Ether]	USD
Whitelist	70254	0.000140508	0.056
Blacklist	77100	0.0001542	0.061
Announcement	34041	0.000068082	0.027
Verification	94375	0.00018875	0.075
Acceptance	95863	0.000191726	0.076
Valuation	164100	0.0003282	0.13

5. Conclusions and Future Work

With the VaNetChain, we have presented a solution to allow robust, reliable, and traceable communications in VANETs, which can provide foundations for the development of new applications that depend on ensuring certain properties for the data generated and transmitted by the vehicles. This is achieved by entwining the blockchain protocols with the architecture and the procedures of a virtualization layer. On the one hand, this serves to overcome the limitations of the consensus and reputation mechanisms presented in the past. On the other, it is the key to guaranteeing proper operation of blockchain technology, whereas previous approaches failed to cope with the challenging environment of VANETs.

The simulation experiments demonstrate the feasibility of the proposal, while reflecting the optimal number of mRSUs to deploy. The effort due to emulating a network of virtual nodes pays off in terms of packet delivery ratios and end-to-end delays. The findings about the density of mRSUs suggest that the mRSUs can be turned on or off depending on the traffic conditions observed at any given moment.

Currently, we are investigating the adoption of the IEEE 802.11bd standard (an evolution of IEEE 802.11p) in our simulation environment, in order to study the impact on VaNetChain performance of having connections with better spectral efficiency, greater reliability and a wider range [66].

Author Contributions: Investigation, P.V.-T.; methodology, P.V.-T. and J.B.-T.; software, P.V.-T., E.O.-M., and P.G.-S.; supervision M.L.-N.; validation, P.G.-S. and E.O.-M.; visualization, P.V.-T.; writing—original draft, P.V.-T. and J.B.-T; writing—review and editing, M.L.-N. and M.R.-C. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been supported by the European Regional Development Fund (ERDF) through the Ministerio de Economía, Industria y Competitividad (Gobierno de España) research project TIN2017-87604-R, and through the Galician Regional Government under the agreement for funding the atlanTTic Research Center for Telecommunication Technologies and its Program for the Consolidation and Structuring of Competitive Research Groups.

Acknowledgments: I would like to express my gratitude to the Universidad Politécnica Salesiana and its Grupo de Investigación en Telecomunicaciones y Telemática (GITEL) for the scholarship granted to study the program of Maestría de Investigación en Telemática (P.V.-T.).

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

References

1. Zhang, D.; Yu, F.R.; Yang, R. Blockchain-Based Distributed Software-Defined Vehicular Networks: A Dueling Deep Q Learning Approach. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *5*, 1086–1100. [CrossRef]
2. Deng, X.; Gao, T. Electronic Payment Schemes Based on Blockchain in VANETs. *IEEE Access* **2020**, *8*, 38296–38303. [CrossRef]
3. Ilarri, S.; Delot, T.; Trillo-Lado, R. A data management perspective on vehicular networks. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 2420–2460. [CrossRef]
4. Kim, S. Impacts of Mobility on Performance of Blockchain in VANET. *IEEE Access* **2019**, *7*, 68646–68655. [CrossRef]
5. Batabyal, A.A.; Beladi, H. The optimal provision of information and communication technologies in smart cities. *Technol. Forecast. Soc. Chang.* **2019**, *147*, 216–220. [CrossRef]
6. Rasheed, A.; Gillani, S.; Ajmal, S.; Qayyum, A. Vehicular ad hoc network (VANET): A survey, challenges, and applications. In *Vehicular Ad-Hoc Networks for Smart Cities*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 39–51.
7. Belli, D.; Chessa, S.; Kantarci, B.; Foschini, L. Toward Fog-Based Mobile Crowdsensing Systems: State of the Art and Opportunities. *IEEE Commun. Mag.* **2019**, *57*, 78–83. [CrossRef]
8. Alamer, A.; Deng, Y.; Wei, G.; Lin, X. Collaborative security in vehicular cloud computing: A game theoretic view. *IEEE Netw.* **2018**, *32*, 72–77. [CrossRef]
9. van der Heijden, R.W.; Dietzel, S.; Leinmüller, T.; Kargl, F. Survey on misbehavior detection in cooperative intelligent transportation systems. *IEEE Commun. Surv. Tutor.* **2018**, *21*, 779–811. [CrossRef]
10. Ni, J.; Zhang, A.; Lin, X.; Shen, X.S. Security, privacy, and fairness in fog-based vehicular crowdsensing. *IEEE Commun. Mag.* **2017**, *55*, 146–152. [CrossRef]
11. Kaffash, S.; Nguyen, A.T.; Zhu, J. Big data algorithms and applications in intelligent transportation system: A review and bibliometric analysis. *Int. J. Prod. Econ.* **2020**, *231*, 107868. [CrossRef]
12. Liu, L.; Chen, C.; Qiu, T.; Zhang, M.; Li, S.; Zhou, B. A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs. *Veh. Commun.* **2018**, *13*, 78–88. [CrossRef]
13. Iancu, B.; Illyes, I.; Peculea, A.; Dadarlat, V. Pollution Probes Application: the impact of using PVDM messages in VANET infrastructures for environmental monitoring. In Proceedings of the 2019 IEEE 15th International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, 5–7 September 2019; pp. 443–449.
14. Rahman, F.I. Impact of V2V Communication on Eco-Route Choice. *LOGI–Sci. J. Transp. Logist.* **2020**, *11*, 37–45. [CrossRef]
15. Liu, X.; Jaekel, A. Congestion control in V2V safety communication: Problem, analysis, approaches. *Electronics* **2019**, *8*, 540. [CrossRef]
16. Eswaraprasad, R.; Raja, L. Improved intelligent transport system for reliable traffic control management by adapting internet of things. In Proceedings of the 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions)(ICTUS), Dubai, UAE, 18–20 December 2017; pp. 597–601.

17. Panagiotou, N.; Zygouras, N.; Katakis, I.; Gunopulos, D.; Zacheilas, N.; Boutsis, I.; Kalogeraki, V.; Lynch, S.; O'Brien, B. Intelligent urban data monitoring for smart cities. In *Joint European Conference on Machine Learning and Knowledge Discovery in Databases*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 177–192.
18. Bhatia, A.; Haribabu, K.; Gupta, K.; Sahu, A. Realization of flexible and scalable VANETs through SDN and virtualization. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 280–282.
19. Shrestha, R.; Bajracharya, R.; Nam, S.Y. Challenges of future VANET and cloud-based approaches. *Wirel. Commun. Mob. Comput.* **2018**, *2018*, 5603518. [CrossRef]
20. Bravo-Torres, J.F.; Ordóñez-Morales, E.F.; López-Nores, M.; Blanco-Fernández, Y.; Pazos-Arias, J.J. Virtualization in VANETs to support the vehicular cloud—Experiments with the network as a service model. In Proceedings of the Third International Conference on Future Generation Communication Technologies (FGCT 2014), Luton, UK, 13–15 August 2014; pp. 1–6.
21. Cui, J.; Wei, L.; Zhong, H.; Zhang, J.; Xu, Y.; Liu, L. Edge Computing in VANETs-An Efficient and Privacy-Preserving Cooperative Downloading Scheme. *IEEE J. Sel. Areas Commun.* **2020**, *38*, 1191–1204. [CrossRef]
22. Guo, J.; Song, B.; Chen, S.; Yu, F.R.; Du, X.; Guizani, M. Context-Aware Object Detection for Vehicular Networks Based on Edge-Cloud Cooperation. *IEEE Internet Things J.* **2019**, *7*, 5783–5791. [CrossRef]
23. Shrestha, R.; Bajracharya, R.; Nam, S.Y. Blockchain-based message dissemination in VANET. In Proceedings of the 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), Kathmandu, Nepal, 25–27 October 2018; pp. 161–166.
24. Cunha, F.; Villas, L.; Boukerche, A.; Maia, G.; Viana, A.; Mini, R.A.; Loureiro, A.A. Data communication in VANETs: Protocols, applications and challenges. *Ad Hoc Netw.* **2016**, *44*, 90–103. [CrossRef]
25. Zheng, D.; Jing, C.; Guo, R.; Gao, S.; Wang, L. A traceable blockchain-based access authentication system with privacy preservation in VANETs. *IEEE Access* **2019**, *7*, 117716–117726. [CrossRef]
26. Lu, Z.; Wang, Q.; Qu, G.; Liu, Z. Bars: a blockchain-based anonymous reputation system for trust management in VANETs. In Proceedings of the 17th IEEE International Conference on Trust, Security And Privacy In Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 98–103.
27. Ma, Z.; Zhang, J.; Guo, Y.; Liu, Y.; Liu, X.; He, W. An Efficient Decentralized Key Management Mechanism for VANET with Blockchain. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5836–5849. [CrossRef]
28. Lu, Z.; Wang, Q.; Qu, G.; Zhang, H.; Liu, Z. A blockchain-based privacy-preserving authentication scheme for vanets. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2019**, *27*, 2792–2801. [CrossRef]
29. Fragkos, G.; Tsiropoulou, E.E.; Papavassiliou, S. Disaster management and information transmission decision-making in public safety systems. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
30. Bravo-Torres, J.F.; López-Nores, M.; Blanco-Fernández, Y.; Pazos-Arias, J.J.; Ordóñez-Morales, E.F. VaNetLayer: A virtualization layer supporting access to web contents from within vehicular networks. *J. Comput. Sci.* **2015**, *11*, 185–195. [CrossRef]
31. Bravo-Torres, J.F.; López-Nores, M.; Blanco-Fernández, Y.; Pazos-Arias, J.J.; Ramos-Cabrer, M.; Gil-Solla, A. Optimizing reactive routing over virtual nodes in VANETs. *IEEE Trans. Veh. Technol.* **2015**, *65*, 2274–2294. [CrossRef]
32. Dai Nguyen, H.P.; Zoltán, R. The Current Security Challenges of Vehicle Communication in the Future Transportation System. In Proceedings of the 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY), Subotica, Serbia, 13–15 September 2018; pp. 000161–000166.
33. Kaur, R.; Singh, T.P.; Khajuria, V. Security issues in vehicular ad-hoc network (VANET). In Proceedings of the 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–12 May 2018; pp. 884–889.
34. Saleet, H.; Langar, R.; Naik, K.; Boutaba, R.; Nayak, A.; Goel, N. Intersection-based geographical routing protocol for VANETs: A proposal and analysis. *IEEE Trans. Veh. Technol.* **2011**, *60*, 4560–4574. [CrossRef]
35. Chahal, M.; Harit, S. A stable and reliable data dissemination scheme based on intelligent forwarding in VANETs. *Int. J. Commun. Syst.* **2019**, *32*, e3869. [CrossRef]

36. Khan, Z.; Fan, P.; Fang, S.; Abbas, F. An unsupervised cluster-based VANET-oriented evolving graph (CVoEG) model and associated reliable routing scheme. *IEEE Trans. Intell. Transp. Syst.* **2019**, *20*, 3844–3859. [CrossRef]
37. Rashid, S.A.; Audah, L.; Hamdi, M.M.; Alani, S. Prediction Based Efficient Multi-hop Clustering Approach with Adaptive Relay Node Selection for VANET. *J. Commun.* **2020**, *15*, 332–344. [CrossRef]
38. Mohammadnezhad, M.; Ghaffari, A. Hybrid routing scheme using imperialist competitive algorithm and RBF neural networks for VANETs. *Wirel. Netw.* **2019**, *25*, 2831–2849. [CrossRef]
39. Bourebia, S.; Hilt, B.; Drouhin, F.; Lorenz, P. A New AODV Based Forecasting Link Breakage Indicator for VANETs. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
40. Joshua, C.J.; Varadarajan, V. An optimization framework for routing protocols in VANETs: a multi-objective firefly algorithm approach. *Wirel. Netw.* **2019**, 1–10. [CrossRef]
41. Huang, X.L.; Ma, X.; Hu, F. Machine learning and intelligent communications. *Mob. Netw. Appl.* **2018**, *23*, 68–70. [CrossRef]
42. Bravo-Torres, J.F.; Lopez-Nores, M.; Saians-Vazquez, J.V.; Blanco-Fernandez, Y.; Pazos-Arias, J.J. An efficient combination of topological and geographical routing for VANETs on top of a virtualization layer. In Proceedings of the 2015 IEEE 81st Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May 2015; pp. 1–5.
43. Ordóñez-Morales, E.F.; Saiáns-Vázquezl, V.; Bravo-Torres, J.F.; Blanco-Fenández, Y.; López-Nores, M. Leveraging proactive and reactive intersection-based routing protocols for collaborative downloading in VANETs. In Proceedings of the 2016 8th IEEE Latin-American Conference on Communications (LATINCOM), Medellin, Colombia, 15–17 November 2016; pp. 1–6.
44. Hussain, R.; Lee, J.; Zeadally, S. Trust in VANET: A Survey of Current Solutions and Future Research Opportunities. *IEEE Trans. Intell. Transp. Syst.* **2020**. [CrossRef]
45. Kothari, A.; Shukla, P.; Pandey, R. Trusit centric approach based on similarity in VANET. In Proceedings of the 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Paralakhemundi, India, 3–5 October 2016; pp. 1923–1926.
46. Sharma, S. Entity-Centric Combined Trust (ECT) Algorithm to Detect Packet Dropping Attack in Vehicular Ad Hoc Networks (VANETs). *Next Gener. Inf. Process. Syst.* **2020**, *2*, 23.
47. Joshua, C.J.; Duraisamy, R.; Varadarajan, V. A reputation based weighted clustering protocol in VANET: A multi-objective firefly approach. *Mob. Netw. Appl.* **2019**, *24*, 1199–1209. [CrossRef]
48. Yao, X.; Zhang, X.; Ning, H.; Li, P. Using trust model to ensure reliable data acquisition in VANETs. *Ad Hoc Netw.* **2017**, *55*, 107–118. [CrossRef]
49. Hussain, R.; Nawaz, W.; Lee, J.; Son, J.; Seo, J.T. A hybrid trust management framework for vehicular social networks. In *International Conference on Computational Social Networks*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 214–225.
50. Kerrache, C.A.; Lakas, A.; Lagraa, N.; Barka, E. UAV-assisted technique for the detection of malicious and selfish nodes in VANETs. *Veh. Commun.* **2018**, *11*, 1–11. [CrossRef]
51. Abassi, R.; Douss, A.B.C.; Sauveron, D. TSME: a trust-based security scheme for message exchange in vehicular Ad hoc networks. *Hum.-Centric Comput. Inf. Sci.* **2020**, *10*, 1–19. [CrossRef]
52. Wang, J.; Wang, Y.; Gu, X.; Chen, L.; Wan, J. ClusterRep: A cluster-based reputation framework for balancing privacy and trust in vehicular participatory sensing. *Int. J. Distrib. Sens. Netw.* **2018**, *14*. [CrossRef]
53. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A threshold anonymous authentication protocol for VANETs. *IEEE Trans. Veh. Technol.* **2015**, *65*, 1711–1720. [CrossRef]
54. Manvi, S.S.; Tangade, S. A survey on authentication schemes in VANETs for secured communication. *Veh. Commun.* **2017**, *9*, 19–30. [CrossRef]
55. Manivannan, D.; Moni, S.S.; Zeadally, S. Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETworks (VANETs). *Veh. Commun.* **2020**, *25*, 100247. [CrossRef]
56. Treleaven, P.; Brown, R.G.; Yang, D. Blockchain technology in finance. *Computer* **2017**, *50*, 14–17. [CrossRef]
57. Lo, S.K.; Xu, X.; Chiam, Y.K.; Lu, Q. Evaluating suitability of applying blockchain. In Proceedings of the 2017 22nd International Conference on Engineering of Complex Computer Systems (ICECCS), Fukuoka, Japan, 5–8 November 2017; pp. 158–161.

58. Singh, M.; Kim, S. Crypto trust point (cTp) for secure data sharing among intelligent vehicles. In Proceedings of the 2018 International Conference on Electronics, Information, and Communication (ICEIC), Honolulu, HI, USA, 24–27 January 2018; pp. 1–4.
59. Lasla, N.; Younis, M.; Znaidi, W.; Arbia, D.B. Efficient Distributed Admission and Revocation using Blockchain for Cooperative ITS. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5.
60. Malik, N.; Nanda, P.; Arora, A.; He, X.; Puthal, D. Blockchain Based Secured Identity Authentication and Expeditious Revocation Framework for Vehicular Networks. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 674–679.
61. 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]
62. Wu, J.; Griffeth, N.; Newport, C.; Lynch, N. Engineering the virtual node layer for reactive MANET routing. In Proceedings of the 2011 IEEE 10th International Symposium on Network Computing and Applications, Cambridge, MA, USA, 25–27 August 2011; pp. 131–138.
63. Singhal, C.; Barik, P.K. Adaptive Multimedia Services in Next-Generation Broadband Wireless Access Network. In *Resource Allocation in Next-Generation Broadband Wireless Access Networks*; IGI Global: Hershey, Pennsylvania, USA, 2017; pp. 1–31.
64. Liu, C.; Huang, H.; Du, H. Optimal RSUs deployment with delay bound along highways in VANET. *J. Comb. Optim.* **2017**, *33*, 1168–1182. [CrossRef]
65. Perez, D.; Livshits, B. Broken metre: Attacking resource metering in evm. *arXiv* **2019**, arXiv:1909.07220.
66. Arena, F.; Pau, G. A Review on IEEE 802.11 p for Intelligent Transportation Systems. *J. Sens. Actuator Netw.* **2020**, *9*, 22. [CrossRef]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.