applied sciences

MDPI

Article

Blockchain Based Trust Model Using Tendermint in Vehicular Adhoc Networks

Sandeep Kumar Arora [1], Gulshan Kumar [2,*] and Tai-hoon Kim [3,*]

1 Department of Electronics and Electrical Engineering, Lovely Professional University, Punjab 144411, India; sandeep.16930@lpu.co.in
2 Department of Computer Science and Engineering, Lovely Professional University, Punjab 144411, India
3 Glocal Campus, Konkuk University, 268, Chungwon-daero, Chungju-si 27478, Korea
* Correspondence: gulshan3971@gmail.com (G.K.); taihoonn@daum.net (T.-h.K.)

Abstract: Blockchain is the consensus-based technology used to resolve conflicts in Byzantine environments. Vehicles validate the messages received from neighboring vehicles using the gradient boosting technique (GBT). Based on the validation results, the message source vehicle generates the ratings that are to be uploaded to roadside units (RSUs), and through that, the trust offset value can be calculated. All RSUs maintain the trust blockchain, and each RSU tries to add their blocks to the trust blockchain. We proposed a blockchain-based trust management model for the vehicular adhoc network (VANET) based on Tendermint. It eliminates the problem of malicious nodes entering the network, and will also overcome the problem of power consumption. Simulation results also show that the proposed system is 7.8% and 15.6% effective and efficient in terms of packet delivery ratio (PDR) and end-to-end delay (EED), respectively, to collect the trusted data between the vehicles.

Keywords: blockchain; vehicles; trust; traffic; consensus

Citation: Arora, S.K.; Kumar, G.; Kim, T.-h. Blockchain Based Trust Model Using Tendermint in Vehicular Adhoc Networks. *Appl. Sci.* **2021**, *11*, 1998. https://doi.org/10.3390/app11051998

Received: 6 February 2021
Accepted: 19 February 2021
Published: 24 February 2021

1. Introduction

The vehicular adhoc network (VANET) is a sub-class of the mobile adhoc network (MANET), which is deployed on the road to make the transport system intelligent. Vehicular communication uses onboard sensing and computation [1,2], as shown in Figure 1.

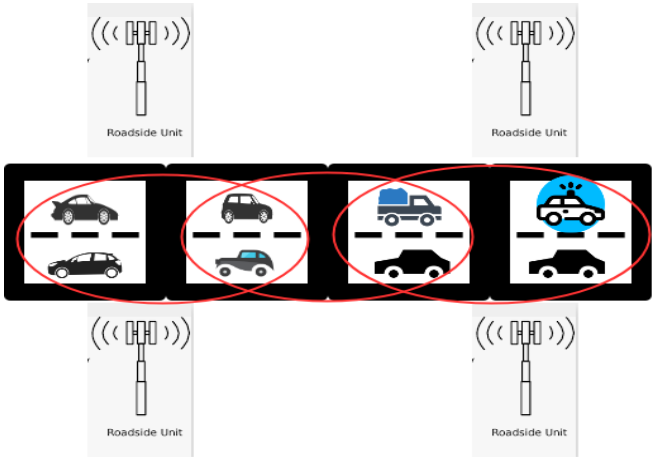

Figure 1. Architecture of vehicular adhoc network (VANET).

Even smart vehicles want to communicate with each other, and this is the basic key in the fifth-generation network (5G) [3,4]. However, due to high mobility and the dynamism of the network, we cannot trust on every vehicle. The malicious nodes can enter the network and spread false information in the network, which leads to the failure of the vehicular

network. For example, a malicious node can broadcast a message that there is an accident on a road, claiming congestion, but there was no accident and traffic congestion. These types of misbehavior produce risk in the vehicular network. Therefore, trustworthiness is an important factor to deal with, which is a critical issue in the network [3].

In distributed systems, byzantine consensus is used to exchange the information between the vehicles using trust management [5]. The vehicular network helps to provide information about road accidents, traffic congestion, road conditions, etc., and this helps the vehicles to be aware of the critical situations, thus improving transportation safety [6,7].

The trust management program allows vehicles to determine whether or not the received message is reliable [8,9]. Normally, the vehicle's trust value can be determined based on the ratings produced by the vehicle's past behavior. Trust management can be categorized into two classes, i.e., centralized and decentralized [10,11]. Centralized systems store confidence values on the central repository, e.g., the cloud repository. These central systems cannot fulfill the stringent quality of services (QoS) specifications because every time node has to ask the central server to test the trust value, which increases the latency of the network. Trust management is to be conducted at the vehicle or RSU level in decentralized trust management systems, so that the burden of interaction with the server is reduced to a great extent, which ultimately increases the efficiency of the system [12–14]. Moreover, we cannot rely on one node for trust management. Due to the dynamic network, it is difficult to trust each node for the ratings. Therefore, designing an effective decentralized network is still a challenge [14]. In [15], the authors has discussed about the families of consensus for the permissioned as well as permissionless blockchain which has been described in the literature.

The proposed system works effectively by retaining the trustworthiness between the nodes in vehicular networks. The internet of vehicles, using big data, is also a trending area, and which explored by game theory, i.e., coalition games for spatial-temporal big data in the internet of vehicles, where the vehicles will be rewarded and penalized according to game rules [16]. Blockchain is one of the new innovations in the financial sector that establishes a clear and tamper-proof ledger without centralized banks, so people can transact with absolute trust [17,18]. Therefore, due to the design of the blockchain's trust management system, it can be conveniently carried out between nodes with decentralized systems [19]. Automated-based contention-aware data forwarding has also been proposed, which is based on Baysian coalition game theory, which improves the routing parameters of VANET [17,20]. The trust between the multiple parties can be generated with the help of Byzantine consensus [21,22]. Due to its high security, blockchain has been commonly used in the non-financial market, i.e., content delivery, key management [23], decentralized storage [24–26], etc. Some popular projects like Hyperledger can also be used as an application of byzantine fault tolerance [27,28]. A blockchain based crowdsourcing program is also defined for the court adjudication [29–31]. The block generation undertaken by the attacker is slow as compared to the normal RSUs, due to the issue of trustworthiness. The benefit of using the cross blockchain through Tendermint is the interoperability between blockchains, which also reduces the latency and improves the transaction speed. The existing technique has worked on the proof of work consensus, which is not at all a power-efficient method. In the proposed method we have implemented the decentralized cross chain Tendermint protocol, in which the transaction speed is greater, and this allows us to use and send the data on any blockchain. The existing study has only shown transactions and ratings, but we also worked on the quality of services and calculated the effect on QoS. Voting-based consensus uses less power as compared to the existing study [32,33]. The contribution of this paper is summarized below:

(a) A decentralized trust management system has been proposed based on blockchain technology, which permits all the vehicles and RSUs to update the trust value in a decentralized manner, and the active participation of all vehicles and RSUs for the updating procedure;

(b) We have proposed a proof of authority (PoA), which is better than proof of work (PoW) and practical Byzantine fault tolerance (pBFT), because of the high energy consumption and greater overhead, respectively.

(c) We have proposed a system model and conducted a simulation which proves that our proposed model is efficient in practical vehicular networks.

2. Related Work

2.1. Byzantine Consensus

The consensus is a part of distributed computing. An agreement is reached between a distributed number of processes [5], and a popular consensus scheme is called Byzantine fault tolerance (BFT). This type of protocol is used to secure the network from node failure. Practical Byzantine fault tolerance (PBFT) [7] is one of the more well-established BFT algorithms since it is based on three rounds prior to the actual agreement. This ensures that 3f+1 nodes are necessary to reach a consensus if we have f Byzantine nodes [7]. In [15], the author discusses well-known families of consensus algorithms for both permissionless and permissioned blockchains, which include proof of work (PoW), proof of stake (PoS), delegated proof of stake (DPoS), proof of burn (PoB), etc. Next generation deployment has carried out and the quality of services (QoS) has been discussed [34]. QoS plays very important role in the vehicular networks which defines how much efficient is the network which is presented [35]. It consists of packet delivery ratio, end to end delay and the throughput has also been discussed in results analysis [36–39]. The self-mining process consumes much amount of power as described [40]. The decentralized key management mechanism has been proposed, which is a lightweight mutual authentication scheme used to prevent many network attacks [41]. Blockchain architecture is used to prevent many network attacks due to its tamperproof environment, and it provides more security to transactions. Moreover, these transactions are transparent on blockchain [42,43].

The distributed consensus in the blockchain creates trust between multiple parties and is referred to as Byzantine consensus [21]. Byzantine consensus is still a research field and is backed by recent advances in blockchain technology. The consensus is broadly divided into proof-based and voting-based. In the proof-based category, bitcoin is the popular one that uses PoW, which requires the miner to solve a difficult problem, and it requires a large number of resources. Moreover, the transactions are very slow, at nearly seven transactions per second. PoS uses stake to determine the mining difficulty, which can be determined as proof for the voting [21]. The proof-based mechanism provides consistency in the network, but suffers from the lower transaction rate and large resource consumption. The novel VANET system model using edge computing is implemented, and it uses an individual session key for each vehicle to prevent interference [39,42]. The RFID-based mechanism provides better authentication and prevents many network attacks, and it uses elliptic curve cryptography to secure the session [37]. Moreover, the Telecare medical information system also used the ECC mechanism for preserving the anonymity of the user, and this has been found to be suitable in cryptography [38]. Even to secure the localization, the same trust-based mechanism is used in a wireless sensors network, which is based on decentralization [44].

The voting-based consensus is more useful for the permissioned blockchain customer, because knowing your customer's methodology nodes will help achieve a consensus over multiple rounds of collective voting. The popular project Hyperledger fabric [27] uses PBFT in its 0.6 version, and R3 Corda employs BFT-SMaRt [28], which is identical to PBFT.

2.2. Centralized Trust Management

So many researchers have contributed a lot of research work in the area of centralized trust management in recent years. Central servers are used to collect, measure and store the trust values of all vehicles, and are believed to be a fully trusted entity not compromised by an attacker [7,10,11]. Vehicles notice traffic-related incidents and issue notices to neighbors.

Vehicle feedback is obtained from a centralized reputation-based server. Based on these results, the server is able to issue certificates based on their credibility values.

Simulation and punishment mechanisms are also shown [10]. In this, the concept of micropayment has been shown. Honest nodes can earn a certain amount of credits, which they can spend on relaying the packets. If any node with greater packet drop is identified by the receiver, it will be evicted from the network.

With the evident increase in the number of vehicles, it is not possible to cope with all nodes using centralized systems. Moreover, if the central system fails, the entire system's failure can be possible.

2.3. Blockchain Based Decentralized Data Management

Blockchain is a very recent technology that also provides the concept of decentralization. A blockchain-based crowdsourcing program introduced by [29] is used to apply for court adjudication. In [30,31] proposed blockchain-based crowdfunding is shown that is a different form of crowdsourcing. In addition, ref. [25] developed a distributed storage and keyword search based on blockchain. The public keys of the entire network are stored in this paper blockchain. Therefore, blockchain helps to design a trust-based decentralized and tamper-proof network for vehicular networks. It has summarized that PoW and PoS are the consensuses that are widely used in permissionless blockchain. Tendermint is the open-source consensus protocol that can solve the problem of Byzantine fault tolerance.

3. Proposed Approach

In the proposed system, the model consists of the following components, as illustrated in Figure 2.

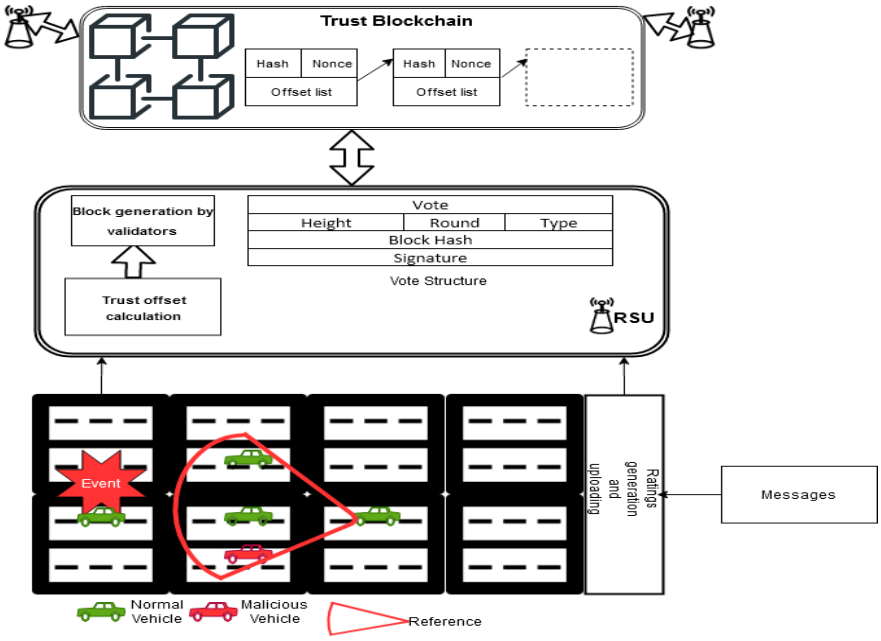

Figure 2. Proposed blockchain-based system model for trust management system.

3.1. Road Side Unit

Roadside units are used to communicate with the vehicles running on the road, and give information and updates about the route. This acts as a bridge between the trusted authority and end-users. Moreover, RSU is also responsible for some of the major tasks, i.e., the collection of ratings and trust value management.

3.2. On-Board Unit

This unit is used to broadcast the traffic-related information periodically. The information contains speed, multimedia, and the updating of the direction for traffic movement.

3.3. Trust Value Management

We assume that the RSUs are able to calculate the trust values by aggregation of the ratings received from the different vehicles. So, the credibility of the message is basically judged by the aggregated value of the rating, and can be fetched from the trust value management servers [32].

3.4. Main Procedures

The proposed model procedure is divided into three parts, as described in Figure 2.

Step 1 Rating generation and uploading

This is the first step towards the decentralization of trust management in a vehicular network. This is the procedure that has to be conducted on vehicles. Some specific rules are required to assess the credibility of the messages and to generate the ratings. The messages are divided into groups {*M1, M2, … … … M_j*}, where M_j represents the group reporting event, e.g., an accident happened in one road segment R. All messages have different values of ratings calculated by the RSUs. The vehicle which is near to the event will have more rating value because it is close to the event and will be exactly aware of whether the event happened or not. Therefore, the credibility of a certain message is defined as follows [32]:

$$c_k^j = b + e^{-\gamma d_k^j} \tag{1}$$

where c_k^j is the credibility of the message in group Mj sent by vehicle, d_k^j is the distance between the sender and the location of the event. b and γ are two preset parameters, which control the lower bound and the rate of change of message credibility. Moreover, $c_k^j = 0$, if k does not report this event. The receiver can obtain a credibility set C^j for event e^j using Equation (1), where $C^j = \left\{ c_1^j, c_2^j, \ldots\ldots \right\}$. Based on credibility set C, the receiver is able to calculate the aggregated credibility of event e using the gradient boosting technique [33].

The gradient boosting technique splits the input space into T_m disjoint regions, such as $R_{1m}, R_{2m}, \ldots R_{Tm}$, and then predicts a vehicle with a lower trust value in each region. Here, T_m represents the number of leaves in a tree. Therefore, this is the output of gradient boosting. Thus, the output of the gradient boosting tree is $h_m(x)$ for input x (x indicates the mobile node with trust value), and this is represented mathematically as follows:

$$h_m(x) = \sum_{T=1}^{T_m} b_{tm}\, I\,(x \in R_{Tm}) \tag{2}$$

From Equation (2), b_{tm} denotes the predicted mobile nodes, which consist of lower trust values in the tree. After that, the coefficients b_{tm} are multiplied by a random value γ_m in order to remove the lower trust value mobile nodes in the VANET scenario. So, the updated model is described below:

$$F_m(x) = F_{m-1}(x) + \gamma_m h_m(x) \tag{3}$$

$$\gamma_m = \underset{\gamma}{\operatorname{argmin}} \sum_{i-1}^{n} L\,(y_i,\, F_{m-1}(x_i) + \gamma_m h_m(x_i)) \tag{4}$$

Using Equations (3) and (4), the lower trust values from the vehicular network will be removed by RSU. Finally, the nodes with higher trust values will be retained by the given formula,

$$F_m(x) = F_{m-1}(x) + \sum_{T=1}^{T_m} \gamma_{T_m} I(x \in R_{Tm}) \tag{5}$$

$$\gamma_{T_m} = \underset{\gamma}{\operatorname{argmin}} \sum_{x_i \in R_{Tm}}^{n} L(y_i, F_{m-1}(x_i)) \quad (6)$$

The RSU may have differences in ratings produced by similar messages, e.g., nine positive and three negative ratings. The former is a majority group, and the latter is a minority group. In the proposed methodology, weighted aggregation solves the problem of ranking conflicts. The offset is between −1 and +1 (normalized value), which is positively associated with the positive rating ratio in this message. The estimation of the offset value of the trust is shown in Equation (7).

$$\sigma_k^j = \frac{\theta_1.m - \theta_2.n}{m+n} \quad (7)$$

where σ_k^j is the trust value offset of vehicle k based on message j and $\sigma_k^j \in [-1, 1]$. m and n are the number of positive and negative ratings, whose weights are θ_1 and θ_2, respectively. θ_1 and θ_2 are determined using Equations (8) and (9), respectively.

$$\theta_1 = \frac{F(m)}{F(m) + F(n)} \quad (8)$$

$$\theta_2 = \frac{F(n)}{F(m) + F(n)} \quad (9)$$

where $F(.)$ controls the sensitivity of the minority group of ratings, e.g., $F(x) = x^2$ is less sensitive to the minority group of ratings compared with $F(x) = x$. This strategy has been carried out under the premise that the intruder cannot dominate the majority group. The proposed weighted aggregation is therefore in a position to boost the reliability of the trust value offsets.

Step 2 BFT based consensus for transaction between vehicles

PoW cannot deter the participants from performing selfish mining [40]. If we choose the PoS, we can remove the problem of energy consumption, and speed can also be increased. The joint proof of work and the method for creating a block takes the number of absolute offsets as a stake, and complexity of it is dependent on the RSU which has more stakes, and can quickly locate the nonce and win the mining election [32] and will publish the block faster as compared to PoW alone, but PoW and PoS both are the mechanisms used for permissionless blockchain, which is more vulnerable to network attacks. So, we want to introduce here the permissioned blockchain consensus in our proposed model, which is more secure than the permissionless blockchain. The proposed block generation method is based on validators and voting power, i.e., Tendermint (consensus without mining).

A. *Validators* Every node has the same weight in the BFT process. In Tendermint, nodes with a non-negative sum of voting power and nodes with a positive voting power are considered as validators. Such participants participate in the consensus through the transfer of signatures and votes to the next generation of blocks.

B. The system model Tendermint consists of three steps (Propose, Prevote, Precommit), and two special steps (Commit and NewHeight).

Obtaining more than two-thirds of commitment requires obtaining commitments from a total of two-thirds of the validators. When commitments for this block have been signed and transmitted by two-thirds of the validators, the block is said to be dedicated by the network. The vote structure is shown in Figure 3.

The three steps that we mentioned take one-third of the total allocated time. Every round takes more time as compared to the previous round, so that consensus is achieved and the block generates.

The proposer is chosen in a round-robin fashion in each round, so that the validators are chosen in proportion to their voting power with frequency. The structure of the proposer is shown in Figure 4.

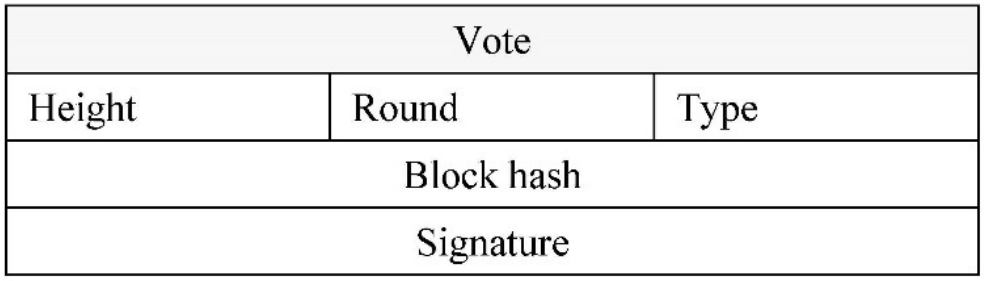

Figure 3. Vote structure.

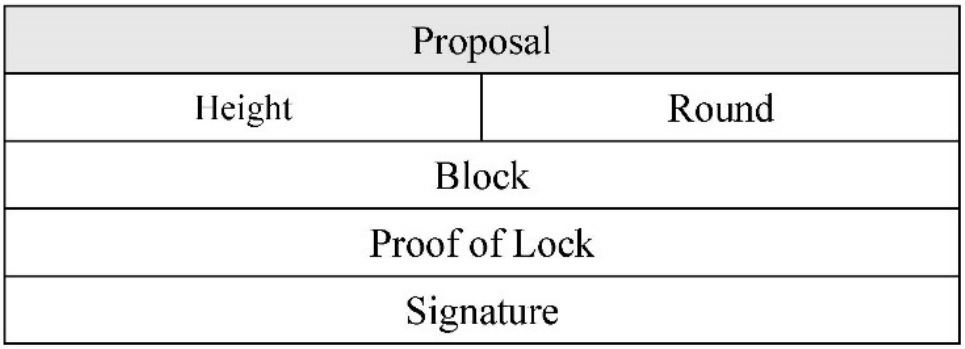

Figure 4. Proposal structure.

The first step is Proposal, in which the proposer transmits a proposal by gossiping to its peer. When a proposer is locked into a prior process, the initiative proposes a proof-of-lock.

In Prevote each validator is determined. If the validator is locked on to any previously proposed block, it will sign and broadcast a locked block prevote. If no block has been sent by the validator then it sends a null prevote.

Each validator makes the decision in the beginning of the Precommit phase. The validator signs and transmits a precommit for that block if it has received more than two-thirds of the prevotes for a similar appropriate block. If the node receives two-thirds null votes, then it simply unlocks the block. Each node makes the decision at the end of the Precommit phase. If more than two-thirds of the precommits have been received by the node, then it is entered for the Commit stage. Otherwise, it will start with Propose in the next round. The Commit step is a very important step here, in which two parallel conditions need to be checked before finalizing the round. First, the node will obtain the block that the network has committed. Second, once received and signed by the validator, it broadcasts a commit for that block. All the workflow is shown in Figure 5, and we have considered that the elements are uniquely located. This is the one round of consensus for the generation of a block by the RSUs. In this way, RSUs can handle the malicious node if any is present in the network.

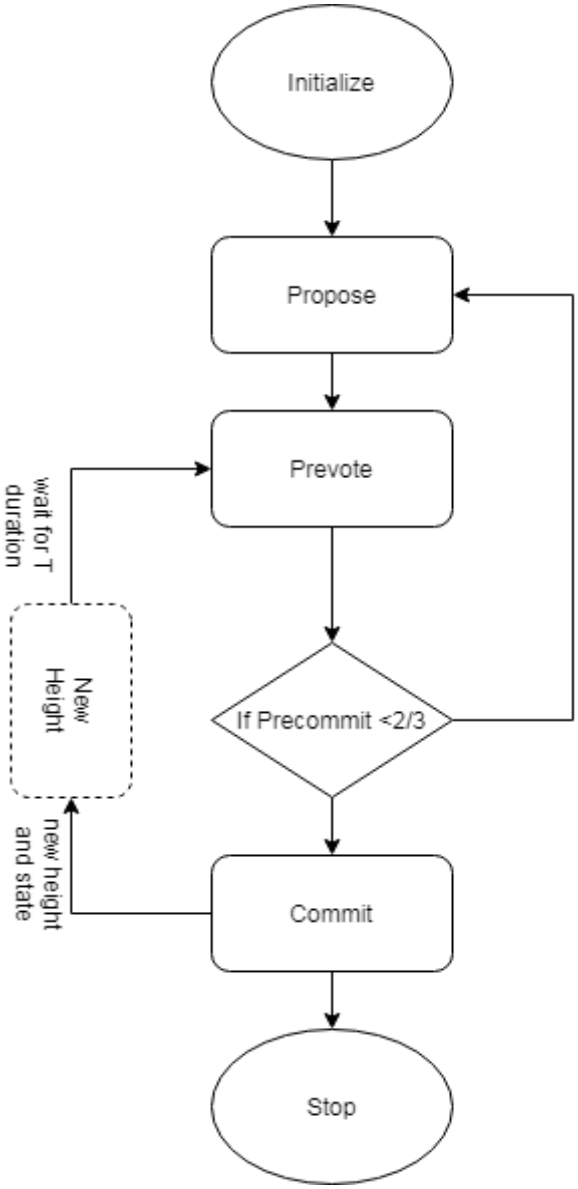

Figure 5. Consensus algorithm without mining used by Tendermint.

4. Simulation Parameters

To analyze the proposed approach, network performance analysis is selected. The proposed consensus scheme performance was also compared with the existing consensus scheme implemented on VANET. Simulator for Urban Mobility (SUMO) has been used for the vehicular setup, and the simulator parameters are as described in Table 1.

Table 1. Simulation parameters.

Parameter	Value
No. of Nodes	50
Maximum Vehicle Speed	40 m/s
Length of Vehicle	3 m
Width of Vehicle	2 m
Number of RSUs	7
RSU coverage	1 Km

5. Implementation and Results

The performance of Tendermint, considering the different numbers of nodes, is shown in Figure 6. In this, we have considered four scenarios in which 50 nodes are considered at the maximum, and it is also shown that Tendermint can process thousands of transactions per second, which ultimately increases the throughput level, and the delay of the system is reduced.

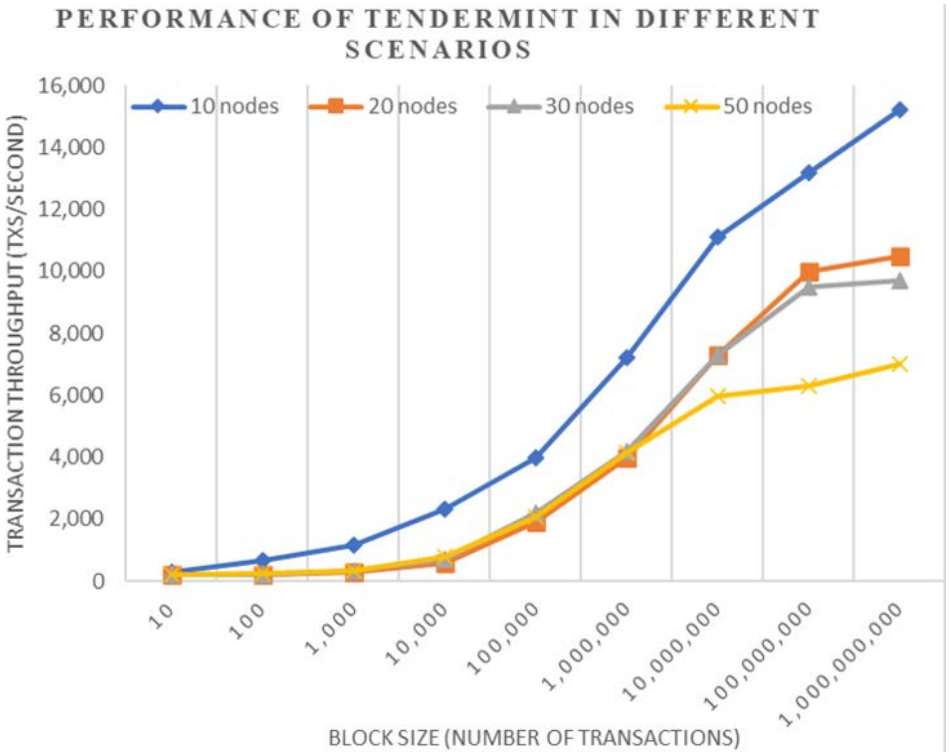

Figure 6. Performance of Tendermint.

5.1. Performance Metrics

This section reflects the theoretical study and the feasibility of the consensus suggested in VANET. The network output is measured in terms of the packet delivery ratio, and the end-to-end delay. Evaluation of the results is achieved by running the simulation, and statistical analysis is conducted by averaging the collected values to a mean value.

5.2. Packet Delivery Ratio (PDR)

This applies to the ratio of packets received successfully to the cumulative number of packets transmitted across the network [35]. Mathematically, it is given by:

$$PDR = \frac{P_r}{P_s} \tag{10}$$

where P_r is the total number of packets received and P_s is the total number of packets sent.

Figure 7 illustrates the packet delivery ratio for the proposed consensus scheme, i.e., Tendermint incurred a higher PDR, improved by 7.8%, 5.6% and 2.4% compared to PoW, PoS and Hybrid, respectively.

5.3. End-to-End Delay

End-to-end delay (EED) is defined as the time it takes for a packet to get from the source to the destination [36,39]. End-to-end delay impacts the PDR significantly on the network. Mathematically, it is given by:

$$EED = \sum T_A - T_S \tag{11}$$

where T_A is the arrival time of the packet and T_S denotes the sent time of the packet.

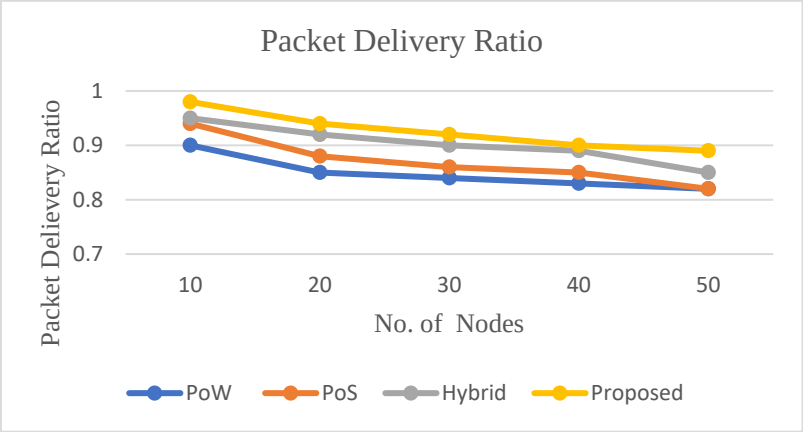

Figure 7. Packet Delivery Ratio.

Figure 8 shows the simulation results, and the proposed solution incurred low end-to-end delay, with a difference of 15.60%, 3.60% and 11.80% compared to PoW, PoS and Hybrid. The average delay in the case of the proposed scheme is 0.15 s, which is far better than other schemes, which are compared in Figure 8.

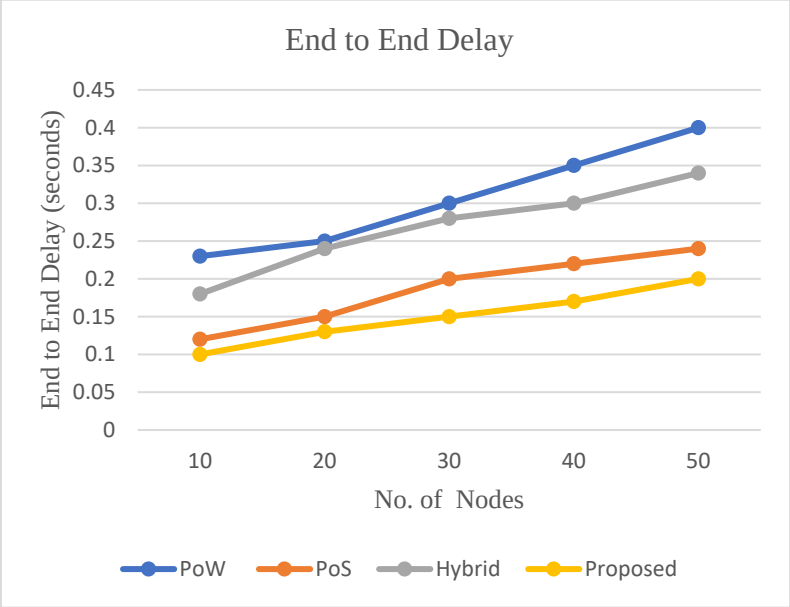

Figure 8. End-to-end delay.

5.4. Performance Analysis of Ratings

As we have already shown, the end-to-end delay is greater in the case of PoW, i.e., it is also reflected in the rating calculation. The latency is shown in Figure 9, and it is low, with a difference of 0.48 s, 0.44 s, and 1.46 s as compared to PoW, PoS and Hybrid.

5.5. Comparitive Analysis of Results

In this section we have analyzed and compared the results, and found that our proposed scheme is more efficient as compared to the literature [32]. Table 2, shown below, gives the comparison.

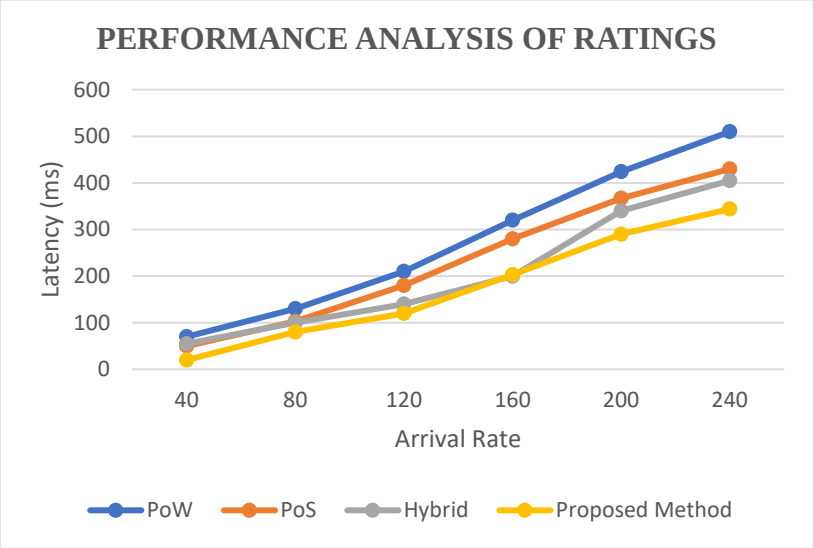

Figure 9. Performance analysis of ratings.

Table 2. Comparative analysis of results.

Consensus Scheme	Latency
1. PoW	High
2. PoS	High
3. Hybrid	Moderate
4. Proposed Scheme	Low

As the traffic increases, the load on the system will increase. The computation power of the RSU should be good enough to process a huge amount of data because the processors in the cars are not that powerful, and this is the reason we have given the computation role to the RSUs.

6. Theoretical Analysis

6.1. Free from Deadlock

This means that no node at any point in time will wait for another node. No node will wait for a separate node to transmit or accept a request, or vote, start to validate a block, or add a block to its line.

6.2. Message Spoofing Attack

This is when a malicious vehicle enters into the system and tries to send fake messages of accidents on the road when there was no accident. This is called message spoofing. We propose the double layer mechanism here to defend against this kind of attack. The first layer will use the gradient boosting technique (GBT), based on machine learning mechanisms, able to provide trustworthiness between the vehicles. The credibility of the message is checked by the receiver, which analyzes the different messages and their ratings broadcasted in the network. Tendermint based on Byzantine fault tolerance acts as a second layer, using the permissioned blockchain, which is much less vulnerable as compared to the permissionless blockchain.

6.3. Overwriting Proposed Blocks

This is when the nodes clash to reject the existing block, and suggest their own new block. To resist this form of attack, after consensus has been achieved, all nodes must agree on the same block to connect to the chain.

6.4. Temperproof Environment

It is difficult to change or tamper the messages stored by the RSUs using blockchain. All the RSUs store the same blockchain version and continuously add new blocks to the blockchain. The involved RSUs will create fake blocks and broadcast them. They do need to contend with the other blocks included in the blockchain, however. Therefore, the amount of compromised RSUs in this case is negligible, due to the use of permissioned blockchain.

6.5. Strong Privacy

Tendermint uses a BFT consensus algorithm, whereby appointed nodes send and receive messages and agree on blocks. It includes Propose, Prevote and Precommit messages. These messages included the signature of the node that created the message. A block will generate after the consensus contains a Precommit signature of the node that agreed on the block. Thus, it maintains the privacy among the nodes.

7. Conclusions

In this paper, we have proposed a blockchain-based decentralized system that maintains the trust between the vehicles, and wherein trust value is aggregated in the RSUs to share the data without tampering, because each of the RSUs stores the same version of the blockchain. Decentralized blockchain mechanisms also secure the messages stored in RSUs, and also maintain the privacy of vehicles. Decentralized systems are very popular in the market, which can be integrated with industry 4.0 to secure their production and manufacturing in industry. Simulations are carried out to check out the performance of the proposed technique, and this shows that the proposed technique provides a high rate of transactions per second, high throughput, and efficient PDR values. In future, the work on scalability can be performed when the number of vehicles grows rapidly, and the transaction speed and latency will be impacted more. We need to see the effect of other consensus protocols on the existing network. It is believed that by applying a blockchain-based system, the vehicles can communicate with neighbors safely, and it also helps to build an intelligent transportation system.

Author Contributions: S.K.A. designed and performed the experiments, derived the models, and analyzed the data. He also wrote the manuscript in consultation with G.K. and T.-h.K.; G.K. and T.-h.K. performed result analysis and supervised the work. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

References

1. Zhou, H.; Liu, B.; Luan, T.H.; Hou, F.; Gui, L.; Li, Y.; Yu, Q.; Shen, X. ChainCluster: Engineering a cooperative content distribution framework for highway vehicular communica-tions. *IEEE Trans. Intell. Transp. Syst.* **2014**, *15*, 2644–2657. [CrossRef]
2. He, S.; Shin, D.-H.; Zhang, J.; Chen, J.; Sun, Y. Full-view area coverage in camera sensor networks: Dimension reduction and near-optimal solutions. *IEEE Trans. Veh. Technol.* **2015**, *65*, 7448–7461. [CrossRef]
3. Zheng, K.; Zheng, Q.; Chatzimisios, P.; Xiang, W.; Zhou, Y. Heterogeneous vehicular networking: A survey on architec-ture, challenges, and solutions. *IEEE Commun. Surveys Tuts.* **2015**, *17*, 2377–2396. [CrossRef]
4. Wasef, R.; Lu, X.L.; Shen, X. Complementing public key infrastructure to secure vehicular ad hoc networks. *IEEE Wirel. Commun.* **2010**, *17*, 22–28. [CrossRef]
5. De Angelis, D.S.; Aniello, L.; Leonardo, B.; Roberto, L.; Federico, M.; Margheri, A.; Sassone, V. PBFT vs proof-of-authority: Applying the CAP theorem to permissioned blockchain. In Proceedings of the Italian Conference on Cyber Security, Milan, Italy, 6–9 February 2018; pp. 1–11.

6. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and privacy in smart city applications: Challenges and solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
7. Castro, M.; Liskov, B. Practical byzantine fault tolerance and proactive recovery. *ACM Trans. Comput. Syst.* **2002**, *20*, 398–461. [CrossRef]
8. Roosta, T.; Meingast, M.; Sastry, S. Distributed reputation system for tracking applications in sensor networks. In Proceedings of the 3rd Annual International Conference Mobile Ubiquitous System, San Jose, CA, USA, 17–21 July 2006; pp. 1–8.
9. Li, S.; Wang, X. Quickest attack detection in multi-agent reputation systems. *IEEE J. Sel. Top. Signal Process.* **2014**, *8*, 653–666. [CrossRef]
10. Mahmoud, M.E.; Shen, S. An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks. *IEEE Trans. Veh. Technol.* **2011**, *60*, 3947–3962. [CrossRef]
11. Lai, C.; Zhang, K.; Cheng, N.; Li, H.; Shen, X. SIRC: A secure incentive scheme for reliable cooperative downloading in highway VANETs. *IEEE Trans. Intell. Transp. Syst.* **2016**, *18*, 1–16. [CrossRef]
12. Gurung, S.; Lin, D.; Squicciarini, A.; Bertino, J. Information oriented trustworthiness evaluation in vehicular ad-hoc networks. In Proceedings of the International Conference Network System Security, Madrid, Spain, 3–4 June 2013; pp. 94–108.
13. Li, Z.; Chigan, C.T. On joint privacy and reputation assurance for vehicular ad hoc networks. *IEEE Trans. Mob. Comput.* **2014**, *13*, 2334–2344. [CrossRef]
14. Huang, X.; Yu, R.; Kang, J.; Zhang, Y. Distributed reputation management for secure and efficient vehicular edge com-puting and networks. *IEEE Access* **2017**, *5*, 25408–25420. [CrossRef]
15. Mattila, J. The blockchain phenomenon. In Proceedings of the Berkeley Roundtable of the International Economy, Berkeley, CA, USA, 24–26 June 2016.
16. Kumar, N.; Misra, S.; Lqbal, R.; Rodrigues, J.J.P.C. Coalition games for spatio-temporal big data in internet of vehicles environment: A comparative analysis. *IEEE Internet of Things J.* **2015**, *2*, 310–320. [CrossRef]
17. Kumar, N.; Misra, S.; Lqbal, R.; Rodrigues, J.J.P.C. Bayesian coalition game for contention-aware reliable data forwarding in vehicular mobile cloud. *Future Gener. Comput. Syst.* **2015**, *48*, 60–72. [CrossRef]
18. Kim, T.-H.; Kumar, G.; Saha, R.; Rai, M.K.; Buchanan, W.J.; Thomas, R.; Alazab, M. A privacy preserving distributed ledger framework for global human resource record management: The blockchain aspect. *IEEE Access* **2020**, *8*, 96455–96467. [CrossRef]
19. Goyat, R.; Kumar, G.; Rai, M.K.; Saha, R.; Thomas, R.; Kim, T.H. Blockchain powered secure range-free localization in wireless sensor networks. *Arab. J. Sci. Eng.* **2020**, *45*, 6139–6155. [CrossRef]
20. Kumar, N.; Iqbal, R.; Misra, S.; Rodrigues, J.J. An intelligent approach for building a secure decentralized public key infrastructure in VANET. *J. Comput. Syst. Sci.* **2015**, *81*, 1042–1058. [CrossRef]
21. Zyskind, G.; Nathan, O.; Pentland, A. 'Sandy' decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 180–184. [CrossRef]
22. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
23. Lei, A.; Cruickshank, H.; Cao, Y.; Asuquo, P.; Ogah, C.P.A.; Sun, Z. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems. *IEEE Internet Things J.* **2017**, *4*, 1832–1843. [CrossRef]
24. Cai, C.; Yuan, X.; Wang, C. Towards trustworthy and private keyword search in encrypted decentralized storage. In Proceedings of the 2017 IEEE International Conference on Communications (ICC), Paris, France, 21–25 May 2017; pp. 1–7. [CrossRef]
25. Cai, C.; Yuan, X.; Wang, C. Hardening distributed and encrypted keyword search via blockchain. In Proceedings of the 2017 IEEE Symposium on Privacy-Aware Computing (PAC), Washington, DC, USA, 1–4 August 2017; pp. 119–128. [CrossRef]
26. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 2084–2123. [CrossRef]
27. Cachin, C.; Vukolic, M. Blockchains consensus protocols in the wild. *ArXiv* **2017**, *1707*, 01873.
28. Clique. Available online: https://github.com/ethereum/EIPs/issues/225 (accessed on 2 July 2020).
29. Federico, A.S. The Crowd Jury, A Crowdsourced Justice System for the Collaboration Era. Available online: https://medium.com/the-crowdjury/the-crowdjury-a-crowdsourced-court-system-for-the-collaboration-era66da002750d8 (accessed on 2 January 2021).
30. Jacynycz, V.; Calvo, A.; Hassan, S.; Sánchez-Ruiz, A.A. Betfunding: A distributed bounty-based crowdfunding platform over ethereum. In Proceedings of the Distributed Computing and Artificial Intelligence, 13th International Conference, Sevilla, Spain, 1–3 June 2016; Volume 474, pp. 403–411.
31. Zhu, H.; Zhou, Z.Z. Analysis and outlook of applications of blockchain technology to equity crowdfunding in China. *Financ. Innov.* **2016**, *2*, 29. [CrossRef]
32. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C.M. Blockchain-based decentralized trust management in vehicular networks. *IEEE Internet Things J.* **2019**, *6*, 1495–1505. [CrossRef]
33. Sangeetha, S.; Sathappan, S. Self-organized gradient boosting key authentication for secured data communication in mobile adhoc network. *Int. J. Appl. Eng. Res.* **2017**, *12*, 7823–7832.
34. *Study on LTE-Based V2X Services, V1.0.0: TSG RAN 3GPP*; TR 36.885; European Telecommunications Standards Institute: Sophia Antipolis, France, 2016.

35. Draz, U.; Ali, T.; Yasin, S.; Shaf, A. Evaluation based analysis of packet delivery ratio for AODV and DSR under UDP and TCP environment. In Proceedings of the 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 3–4 March 2018; pp. 1–7.
36. Shorfuzzaman, M.; Masud, M.; Rahman, M. Characterizing end-to-end delay performance of randomized TCP using an analytical model. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 406–412. [CrossRef]
37. Kumar, N.; Kaur, K.; Misra, S.C.; Iqbal, R. An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud. *Peer Peer Netw. Appl.* **2015**, *9*, 824–840. [CrossRef]
38. Amin, R.; Islam, S.K.H.; Biswas, G.P.; Khan, M.K.; Kumar, N. An efficient and practical smart card based anonymity preserving user authentication scheme for TMIS using elliptic curve cryptography. *J. Med. Syst.* **2015**, *39*, 180. [CrossRef]
39. Pukale, P.; Gupta, P. Analysis of end-to-end delay in vehicular networks. *Int. J. Sci. Res.* **2015**, *5*, 1122–1125.
40. Thin, W.Y.M.M.; Dong, N.; Bai, G.; Dong, J.S. Formal analysis of a proof-of-stake blockchain. In Proceedings of the 2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS), Melbourne, Australia, 12–14 December 2018; pp. 197–200.
41. 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]
42. Tan, H.; Chung, I. Secure authentication and key management with blockchain in VANETs. *IEEE Access* **2019**, *8*, 2482–2498. [CrossRef]
43. Khan, A.S.; Balan, K.; Javed, Y.; Tarmizi, S.; Abdullah, J. Secure trust-based blockchain architecture to prevent attacks in VANET. *Sensors* **2019**, *19*, 4954. [CrossRef] [PubMed]
44. Kim, T.H.; Goyat, R.; Kumar, G. A novel trust evaluation process for secure localization using a decentralized block-chain in wireless sensor networks. *IEEE Access* **2019**, *7*, 184133–184144. [CrossRef]